5Rights

5Rights Foundation's Response to the Information Commissioner's Call for Evidence

Age Appropriate Design Code

CONTENTS

INTRODUCTION

5Rights exists to ensure that children's rights are observed online. Children's rights are not optional, however inconvenient. A fair and equitable data protection regime that respects the rights and privileges of childhood will restore trust in a sector that has not adequately responded to the needs and rights of children. The Age-Appropriate Design Code ("the Code") presents the opportunity to re-design children's online experience in a way that meets their needs and mirrors the protections and rights that they are afforded in all other contexts. It is both necessary and desirable for children to engage with the digital environment, but it is the duty of all stakeholders to create an environment in which they can do so creatively, knowledgeably and fearlessly. We therefore welcome the Commissioner's call for evidence.

Our response has been developed following consultation with a large number of organisations and individuals, both in the UK and internationally. 5Rights' network is multidisciplinary and includes; computer scientists; engineers; legal academics and practitioners; designers; privacy experts; technology companies; industry bodies; academics; politicians and policy makers; NGO's; children's charities; child protection experts; child development experts; teachers; parents; and children of many ages. We are grateful for the scale of their interest, expertise and input.

We conclude that the Code should set out a number of clearly articulated principles to guide both the design of online services "likely to be accessed by children" (those under 18), and the regulator's enforcement regime.

5Rights recommends;

The following 10 Guiding Principles should form the basis of the Code:

1 In determining standards and what measures must be taken, the best interests of the child must be the paramount consideration
2 A high bar of privacy by default; i.e. safety by design, privacy by design and high privacy by default should be the norm for all products and services' features and functionalities *likely to be accessed by children*
3 Responsibility for data protection rests with online services, not the child
4 Responsibility for enforcement rests with the regulator, not the child
5 The impact of service design on children (under 18) must be considered in advance
6 The Code must reflect and/or enhance, never lessen, existing regulations, legislation, international agreements and cultural norms that protect children in other contexts, by incorporating and applying them so that they are enforceable in the digital environment
7 The Code must give clarity to the General Data Protection Regulation's ("GDPR") assertion that "children merit specific protection"
8 The Code must reflect and address the needs and concerns articulated by children themselves
9 That children have different needs at different ages and stages of development and these must be considered when designing services
10 Online services have a duty to uphold the spirit as well as the letter of the Code

In addition to establishing the principles by which all stakeholders must act, the Code must clearly set out the Information Commissioner's expectations for the design of online services. 5Rights' recommendations focus on how the overarching principles should apply in practice. To implement our proposals, online services do not need to rely on new forms of technology, rather on a change of design norms and an acceptance of responsibility towards children, backed by corporate will.

We welcome the Commissioner's call for evidence and the opportunity of the Age-Appropriate Design Code to institute a high level of data protection for children.

A summary of our understanding of key terms and concepts can be found in Appendix A.

CHILDHOOD DEVELOPMENT STAGES

The Data Protection Act 2018 ("DPA") requires the Commissioner to take account of the development needs of children at different ages when drafting the Code. The proposed age ranges are as follows: 3-5, 6-9, 11-12, 13-15,16-17.

Q1. In terms of setting design standards for the processing of children's personal data by providers of ISS (online services), how appropriate do you consider the above age brackets would be?

11 Very appropriate

Q1A. Please provide any views or evidence on how appropriate you consider the above age brackets would be in setting design standards for the processing of children's personal data by providers of ISS (online services).

12 Childhood is a journey from dependence to autonomy. Children, therefore, are not a homogenous group; their needs differ according to their age and development stage. Aligning children's services and experience to their development stage is a legal and social norm followed in, for example, education,[1] crime,[2] criminal proceedings[3] and content regulation.[4]

13 There is a danger that proposing age groups may be interpreted as a demand for an 'age-banded Code'. 5Rights does not consider this the right approach. Having regard to children's different needs at different ages[5] should be a basic tenant of design of service.

5Rights recommends

14 A requirement, within the Code that ISS must;

- Consider the needs and "best interests" of children in each individual age group likely to access their service
- Take steps to meet those needs in the default design of services
- Be able to account for the decisions they took with supporting evidence

And for the Commissioner and/or the Court, when enforcing the Code, have regard to the;

- Age groups of children "likely to access" an ISS
- Steps the ISS has taken to meet the "best interests" of those children
- Evidence the ISS has put forward

This would substantially reduce both the accidental or wilful design of services that do not offer sufficient data protection for children of different ages.

Q2. Please provide any views or evidence you have on children's development needs, in an online context in each or any of the above age brackets.

15 Characteristics associated with child development are non-specific to the digital environment, or to any particular child, gender, socioeconomic, ethnic or regional background. What they offer is an overall understanding of the capacity and skills a child might be expected to have at each stage of development, i.e. at a broadly similar age, thereby offering a guide to their capacity for interacting with instructions, information, choices and concepts relating to the use of their data. Appendix B sets out an overview of development capacity in the age ranges set out by the Information Commissioner.

16 **5Rights recognises the evolving capacity of children in different age groups and welcomes the development stages as set out by the Commissioner.**

THE UNITED NATIONS CONVENTION ON THE RIGHTS OF THE CHILD

The Data Protection Act 2018 requires the Commissioner to take account of the UK's obligations under the UN Convention on the Rights of the Child ("UNCRC") when drafting the Code.

Q3. Please provide any views or evidence you have on how the Convention might apply in the context of setting design standards for the processing of children's personal data by providers of ISS (online services).

17 The UNCRC was signed in the UK in 1990.[6] Changes brought about by digital technologies are not yet formally recognised in its articles, however it is widely understood that rights are not context specific.[7]

18 Article 3 is the overarching right of the child that states that in all actions concerning children "the best interests of the child shall be a primary consideration".[8]

19 Additionally, the following General Comments relating to Article 3 are relevant to the Code;

- No.14 (2013) promotes the "full respect of children as rights holders" and provides that a child's best interests may be "the paramount consideration"[9]
- No. 20 (2016) asserts that the implementation of the rights of children should take account of "children's development and their evolving capacities"[10]
- No 20 (2016) cautions that "generic policies designed for children and young people often fail to address adolescents... and are inadequate to guarantee the realisation of their rights. The costs of inaction and failure are high; the foundations laid down during adolescence in terms of emotional security, health, sexuality, education, skills, resilience and understanding of rights will have profound implications, not only for their individual optimum development, but for present and future social and economic development" [11]

20 Of the other 54 articles that make up the UNCRC, the following are of particular interest in relation to data protection; [12]

- Article 2 states that children have the right not be discriminated against
- Article 5 requires States to respect the responsibilities, rights and duties of parents or carers to provide appropriate direction and guidance in the exercise of the child's right, in accordance with their evolving capacities
- Article 6 places States under a duty to ensure the development of the child to the "maximum extent possible"
- Article 12 provides children with the right to express their views in all matters concerning them
- Article 13 gives children the right to freedom of expression, including to seek, receive and impart information and ideas of all kinds
- Article 16 prohibits arbitrary or unlawful interference with a child's privacy
- Article 17 ensures that a child has access to information and material, and sets out the requirement for States to encourage age-appropriate guidelines for the protection of a child from information and material that is injurious to their wellbeing
- Article 31 provides children with the right to rest and leisure time

21 In 2017, the UN Human Rights Council passed a resolution that noted "violations and abuses of the right to privacy in the digital age may affect all individuals, including with particular effects on...[certain groups including] children..."[13]

22 **5Rights welcomes the inclusion of the UNCRC within the Code, specifically that the "best interests" of the child are the paramount consideration in forming a data protection Code for children. It also serves to clarify for others that a child is any person under 18.**

ASPECTS OF DESIGN

We have answered Questions 4 – 5D for each aspect of design, however our answers are predicated on the proposal that the 10 Guiding Principles (paragraphs 1 - 10) form the basis of the Code and apply to each aspect.

Please provide any views or evidence:
Q4. You think the Commissioner should "have regard to" when explaining the meaning and coverage of these terms in the Code.
Q5A. About the opportunities and challenges you think might arise in setting design standards for the processing of children's personal data by providers of ISS (online services), in each or any of the above areas.
Q5B. About how the ICO, working with relevant stakeholders, might use the opportunities presented and positively address any challenges you have identified.
Q5C. About what design standards might be appropriate (i.e. where the bar should be set) in each or any of the above areas and for each or any of the proposed age brackets.
Q5D. Examples of ISS design you consider to be good practice.

DEFAULT PRIVACY SETTINGS

Meaning

23 Privacy settings determine the extent to which a child's personal data is processed by an ISS, including how it can disseminate such data to its wider network of group companies, subcontractors and affiliates, to its clients including advertisers, to other customers (both known and unknown), and to third parties such as public authorities (e.g. school, health services) or third sector and commercial companies. Privacy settings dictate what personal data may be processed, i.e. collected, used and shared, and how long personal data can be held.

24 Privacy is typically set by a combination of:

- Terms and conditions and/or privacy notices
- Norms of a particular service
- Choices made by the user in device and service settings
- Software design
- Parental controls
- Predetermined settings in shared and smart environments, e.g. public Wi-Fi, hotspot, sensors and smart homes

25 Default privacy settings are the privacy settings if a user takes no action to change them, or if the user cannot change them.

Challenges for children

26 **Default settings determine the data privacy of the vast majority of users, including children.** Users very rarely deviate from default settings and 95% never change their privacy settings .[14] For example, 10% of 12-15-year olds amend their settings to use a web browser in privacy mode,[15] and only 18% change their profile settings on social media.[16] Children also experience consent fatigue when repeatedly asked to tick boxes and agree to things when browsing on different sites. Consent is viewed as a chore rather than something meaningful. The outcome is that children do not review terms or notices, so the default privacy settings apply. Most often that default affords the least privacy protection.[17]

27 **Default settings are onerous to change**
During Mark Zuckerberg's appearance before the Senate's Commerce and Judiciary Committee,[18] it was noted that Facebook allows for high privacy settings, but the user "really has to work at it." When asked to "commit to changing all user default settings to minimize to the greatest extent possible, the collection and use of user's data", Mark Zuckerberg was unwilling to commit Facebook to doing so voluntarily.

28 **If users do change privacy settings,[19] tech updates often return to settings to default, meaning that users are forced to check and reset them repeatedly[20]**

29 **Concepts of data privacy are poorly understood by children**
Anne Toth, ex-Head of Privacy at Google and ex-Chief Trust Officer at Yahoo, suggests that a "privacy violation is when my expectations have been violated."[21] However, children should not be expected to understand what constitutes data privacy.[22] For example, they may not know how ISS harvest their personal data, that a service may continue to collect data even once they have navigated away from it[23] or be aware of the vast breadth of personal information being collected (Appendix A).

30 **Children overestimate their online privacy**
Despite neither checking[24] nor changing[25] default privacy settings, many children feel their 'online worlds' on a personal device are private zones.[26] However, personal information is routinely and broadly collected. For example, Facebook collects a complete log of telephone calls and texts, including time and date, numbers called and duration, and whether or not the user is actively using its service.[27] Since most children do not understand the extent to which data is shared (paragraphs 139 - 141), they are also unlikely to appreciate how their personal data is used to track, monitor, interpret or influence their behaviour.[28] In 5Rights' work, we often find that once the implications of data privacy are explained to children, they express concern and some outrage about current practices, and themselves call for greater privacy.[29]

31 **Developmentally, children are unable to anticipate and evaluate the consequences[30] of data processing[31]**
The ability to understand and weigh up long-term consequences doesn't emerge until late teens. It develops unevenly and is typically not fully developed until an individual reaches their 20s.[32] Therefore, a child is unlikely to understand the consequences of data processing, nor take steps to militate against extensive collection and other types of processing. For example, aggregating data sets allows inferences to be made that may impact their ability to access employment, social welfare and credit.[33]

32 **Default privacy settings favour data collection**
ISS have a financial interest in keeping privacy settings at the minimum level (paragraphs 138, 152). Services widely used by children, even children under the age of 13,[34] such as Instagram and Twitter, set profile pages public by default.[35] UKCCIS found that 42% of child social media users knew they had a public profile, and a further 26% did not know the difference between a public or private profile.[36]

The Norwegian Consumer Council's report *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us From Exercising Our Rights to Privacy* found that default settings are used by many companies, including Facebook, Google and Microsoft to manipulate users, and to nudge them towards the most privacy intrusive options. The Council determined this was "unethical" and not in accordance with principles of data protection by default and by design. It found the platforms' privacy settings: [37]

- Are privacy intrusive by default
- Use misleading words that omit or downplay key information
- Offer more limited control of privacy and data than initially appears
- Hide privacy-friendly choices and obscuring settings
- Create choice architecture where choosing the privacy-friendly option requires significantly longer processes
- Dashboards are difficult to navigate, "more resembling a maze than a tool for user control"
- Present users with take it or leave it choices, including no ability to freely postpone decision-making and threatened loss of functionality or deletion of account if the privacy intrusion option was not chosen

33 **Children's personal data creates an indefinite legacy**
The long-term effects of permanent data gathering are not yet known. Childhood is a time of rapid development. There is an inevitable disconnect between an enduring online identity or footprint, and the older self to whom the identity or footprint is still connected. For example, the UK's first Youth Police and Crime Commissioner, Paris Brown, resigned from her post following criticisms of messages she posted on

Twitter between the ages of 14 and 16.[38] Similarly, many called for Mhairi Black, a member of the SNP and youngest MP in the UK, to be sacked after comments she made on Twitter as a teenager were revealed.[39]

34 **Emerging technologies increase the amount of data being collected by default**
Children increasingly live in a world of Internet of Things ("IoT"). Colloquially referred to as smart toys, smart homes, smart classrooms and smart cities; networked devices collect and process data in multiple environments. Connected baby monitors, voice-controlled TVs and toy dolls are able to continuously record and stream video and audio information to data centres[40] in ways that are opaque to children and/or parents.[41] For example, a 2017 report *#WatchOut*[42] found that three out of four smart watches worn by children allowed strangers to track and communicate with the child. Additionally, WIRED found that user's activity data, publicly available through fitness tracker Strava, could be linked to the names of individuals.[43] In a recent report, Which? found that the smart TV they tested, connected to 700 different IP addresses in 15 minutes[44].

Robot design of toys, the rise of voice controls, rises in biometric data collections[45] and affective computing,[46] allow companies to understand very intimate details of a child's life (often more than the child or parent themselves) in a way that was previously impossible and is yet to be fully understood.

35 **Biometric or voice-activated services take increasingly intimate personal data**
For example, sentiment data (emotional state) captured by home assistants;[47] heartbeat and pulse taken whilst playing games;[48] or the development of affective computing methodologies that will monitor the emotional state of drivers and their passengers.[49]

36 **Many internet-connected devices lack "even basic cyber security provisions"**[50]
The Department for Digital, Culture, Media and Sport's report *Secure by Design* (2018) found that:

- Privacy concerns are given too low a priority in the design process[51]
- Manufacturers and suppliers have few incentives to prioritise built-in security[52]
- High expectations are placed on consumers to proactively protect their devices and their privacy, including changing default passwords, updating devices and "opting-out" of sharing their personal information, with limited access to clear and relevant information to enable them to make informed purchasing decisions[53]
- Common default usernames and passwords set by manufacturers are frequently identified as weaknesses in IoT products[54]
- Some products designed specifically for children have had security issues that left voice recordings and images (that families believed were private) open, and available to the public, or easily accessible[55]

5Rights recommends

37 **The Code should require ISS to provide a high bar of data privacy by default**[56]
This would reverse current industry norms and would ensure a child's privacy was safeguarded as standard. In the subsequent section, 5Rights sets out its recommendations for default high privacy standards for each aspect of design. The default high setting must allow a child to use the service in a meaningful way and service design must not include deliberate attempts to encourage a child to open up default settings that are not in his or her "best interests".

Additionally

38 **The privacy standards of online services should be rated and labelled, for example, using a traffic light system**
The BBC and the BBFC use icons and age ratings to provide content advice.[57] The Food Standards Agency uses a traffic light system to provide consumers with nutritional information.[58] A similar approach could be taken to privacy ratings. The Commissioner would set criteria to determine an online service's privacy rating and would also judge compliance with its published rating thereby transferring the responsibility from the child to the ISS and regulator.[59]

39 **Rating and labelling of default privacy settings should be standardised so they become familiar to a child (and parents) as they go from one service to another**

This does not mean that privacy settings cannot be designed within brand and character of the service. This does mean that there would be clarity about what the privacy offer is. Criteria to be determined by the Commissioner.

40 **Guidance on privacy by design for developers should be published**
The digital experience of those with disabilities has been transformed since the universal adoption of accessibility design standards online.[60] Australia's e-safety Commissioner is developing a 'Safety by Design' framework that is grounded in children's rights and will harness industry's responsibility to safeguard its users at the outset and before they are released to the market.[61] Privacy by Design standards within the Code would be equally transformative for children's privacy in the digital ecosystem. This approach has particular relevance for SMEs and start-ups who may have limited developer resource.

41 **Children should have the ability to change settings, but as they do so, the impact of decisions (to open or reinstate restrictions) must be made clear in language suitable for the youngest user group routinely accessing an ISS**
Even if the youngest users are below the online service's official joining age.

42 **Settings must revert to default high once a child logs out or navigates away from a service**

43 **High privacy settings must not be used to unnecessarily restrict or block children from services**

44 **The ICO should consider precautionary measures and guidance for new technologies**
Being mindful of the speed at which new technologies can emerge, the Council of Europe recommends precautionary measures, including assessing on a regular basis any risks of harm that these may pose to children's health, despite the absence of certainty at that time with regard to scientific and technical knowledge of the existence or extent of such risks.[62] In particular, the Commissioner might consider the implications of affective computing (which gathers data about emotional state),[63] or tools such as watches,[64] in order to determine what level of intimate data gathering is permissible and/or in a child's best interests.

DATA MINIMISATION STANDARDS

Meaning

45 Data is generated and collected from individuals through almost every action online. The GDPR states that data minimisation is the principle of restricting what is collected to that which is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"[65]. This principle applies to data collected directly from the user, as well as data collected by third parties, including data which is observed, derived or inferred when tracking a user's activities or combining data sets.

46 **Among the more visible data collection strategies are:**

- Signing up to services and accepting terms and conditions
- Customer service interactions (including Interactive Voice Response applications)
- Online and mobile questionnaires
- Chatbots
- Searching
- Transactional Data
- Logging in
- Sharing content (images, videos, location)
- Commenting (e.g. liking, commenting, retweeting)

47 **Among strategies less understood by a user, particularly a child, are:**

- IoT sensory/actuator data[66]
- Radio Frequency Identification Tags ("RFID")[67]

- Cookies
- Fingerprinting[68]
- Tracking Pixels[69]
- Entity Tags (known as "E-Tags")[70]
- Browsing history
- Internet connection
- Microphones
- Cameras (including video and recording)
- Global Positioning Systems ("GPS")
- Keystroke logging
- Metadata
- Social media
- Loyalty cards
- Gaming apps, e.g. Apple Game Center app
- Satellite imagery
- Employer databases
- Email providers, i.e. Google and Yahoo

Challenges for children

48 **The scale of data collection is not apparent to children**
Appendix C sets out the data routinely collected from children on some popular sites.

49 **Children cannot be expected to determine what level of data collection is proportionate or necessary**[71]
For example, some schools threaten that a child will not be able to enrol without supplying information including a child's ethnicity, service child status, language or Special Educational Needs provision,[72] and yet it may not be necessary, legal or in a child's best interest to give it.

50 **Unfettered collection of personal data allows services to build extremely detailed profiles about their users**
Companies collect ever-greater amounts of data about their users.[73] Data includes a child's communications, interests, contact with others, emotional reactions, facial expressions, purchases and vital signs,[74] revealing a child's relationships, movements, connections and patterns of behaviour.[75] Detailed profiling makes children vulnerable to outside influence and may contravene their rights (paragraphs 105 – 107, 110 - 111). Increasingly, data is collected at scale in all childhood contexts. For example, school data collection includes; what students buy, their attainment, technical devices used, building access times, sickness and profiling of attainment and behaviour, the collection of which is "routine and part of everyday delivery of education in England."[76]

51 **There are few data minimising choices available**
Children cannot be expected to determine what level of data collection is proportionate or necessary.[77] Only 31% of sites/apps offer controls to limit the collection of personal information from children.[78] Most ISS define their services and products very broadly, which obfuscates that only partial or temporary data collection is necessary for a particular function. Even ISS that require payment, including Netflix and Amazon have onerous data collection policies and few data minimising choices available for child users.

52 **Data is held for longer than is necessary**
Online, privacy policies (which form part of terms and conditions; paragraph 68) often state that data is held for a vague and unspecified time period. For example, Pokemon Go keeps data for "as long as we need to provide the Services to you and fulfil the purposes set out in this privacy Policy", Amazon says "as long as required",[79] and EA Games "as long as reasonably necessary to provide you services, create and improve our products, comply with the law and to run our business", without specifying how long this is.[80] Some online services reserve the right to retain data even when the account is closed, for example, Playstation.[81]

53 **Data is shared widely between products and services**
For example, Google's terms and conditions allow routine sharing of data across: Android Auto, Android Messages, Android OS, Android One, Android Phones, Android Tablets, Calendar, Cardboard, Chrome, Chrome Web Store, Chromebook, Chromecast, Contacts, Daydream View, Docs, Drive, Earth, Finance, Forms, Gboard, Gmail, Google Alerts, Google Allo, Google Cast, Google Classroom, Google Cloud Print, Google Duo, Google Expeditions, Google Express, Google Fit, Google Flights, Google Fonts, Google Groups, Google Home, Google One, Google Pay, Google Play, Google Play Apps, Google Play Games, Google Play Movies and TV, Google Play Music, Google Store, Google Street View, Google Wi-Fi, Google for Education, Google+, Hangouts, Inbox by Gmail, Keep, Maps, News, Photos, Pixel 2, Play Protect, Project Fi, Scholar, Search, Sheets, Sites, Slides, Tilt Brush, Translate, Trips, Voice, Waze, Wear OS by Google, YouTube, YouTube Gaming, YouTube Kids, YouTube TV.[82]

54 **Children give more data points than adults**
Data gathering on those using mobile devices is more precise than for those using computers.[83] Since children disproportionately access ISS by mobile devices, they are routinely giving up more data. In 2017, 86% of 12-15 year olds used a smartphone regularly,[84] compared to a laptop or computer (39%).[85] 86% of 3-4 years old's have access to a tablet.[86]

55 **Parents are often unaware of the privacy risks of shared and communal devices**
Smart systems are already present in our homes and workplaces (toys, TVs, security systems, etc.) and gather data, often without engaging the data subject. For example, Alexa; whilst signing-up requires consent to data privacy settings, there is no distinction made between data gathered from children and adults.[87] The data implications of monitoring voices and instructions cannot reasonably be expected to be understood by children in the home nor those children who visit, especially when they see parents talking to virtual assistants and are encouraged to do so themselves.

Parents are often unaware of data privacy in relation to IoT devices. Nor do they consider the privacy settings on devices that might gather data about children under adult contracts and agreements, for example, with their broadband provider. Many children receive 'hand-me-down' phones as parents or older siblings upgrade, with no corresponding tightening of data privacy control.

5Rights is concerned that the failure of online services to provide data minimisation by default, creates security risks that can be used to sexually exploit children. A report from the Internet Watch Foundation documents 2000 cases where children had live-streamed videos of themselves via their webcam, mobile or tablet. In many cases, the report found that "the children appeared to be completely unaware a recording was being made."[88]

56 **Data can create misleading profiles of children**
Commercial data gathered on children may be used to infer preferences, beliefs and behaviours that are inaccurate and create a record of their activities that may be unwanted or unjust (paragraph 106 - 107). So too for education and health data. For example, the Department for Education sells extensive and identifiable personal pupil data (including sensitive, personal data) to commercial companies.[89] The scale on which data is collected from pupils means that mistakes and inaccuracies are inevitable. Even if correct, inferences may reinforce existing prejudices, unfair assumptions and stereotypes.

5Rights recommends

57 **Data processing must be determined by, and aligned to, a child's exact use of a service**
So that children can use individual products and only give or lend (i.e. subject to expiry notice) data to perform those actions necessary to perform a specific service. For absence of doubt, this would prevent sharing between companies within a single entity, between entities and within the different strands of a single company, unless proven to be in the best interests of the child. For example, a child may wish only to use Google's search tool and could instead be offered a private window with a correspondingly narrow data collection and no dissemination.

Additionally

58 **Data minimisation must be by design, and not require arduous or additional user management**

59 **The use of 'catch all' purposes should be prevented**
Phrases used to allow essentially unlimited data collection such as; "provide, troubleshoot, and improve services",[90] "communicate with you",[91] "connect you with people and organisations that you care about",[92] "make recommendations and suggestions to you and other users"[93] should be prohibited. For example, automated voice analysis used to detect when a user is vulnerable to "improve communication",[94] is better understood as "by tracking your vocal stress we are able to identify moments at which you will be most vulnerable to commercial offers."[95]

60 **Data expiry, data caps and time limits should be introduced as standard**
Routine use of data expiry (with a much shorter expiry time) would allow online services to temporarily collect children's data to perform a service, which would then expire as they log-out or navigate away, and/or offer time-limited data collection in the "best interests" of the child. The Commissioner may wish to consider recommending caps and time limits for the collection of children's data by ISS in a similar (but inverse) manner to the way mobile operators quantify and restrict their customers' access to data.

61 **A child's data must only be taken during active use of ISS**
Data collection should cease at the first of; logging off, navigating away, quitting the screen, closing app, etc.

62 **Mandatory deletion of data should be the expectation when a child closes or stops using an account**
It must be opt-in to saving data when deciding to leave/delete an online service. If no action is taken, the ISS must delete the remaining data. An account that has been inactive (i.e. proactively by the child) for more than six months should be considered closed and subject to the above.

63 **The Code should provide guidance on how to balance public benefit against the best interests of individual children**
Health data collection might be considered to be in the best interests of a child, and society more generally. However, the recent sale of NHS data to Deep Mind[96] raises questions about the implications of sharing highly personal data with a commercial company and the extent to which a child has any meaningful choice. Similarly, concerns have been raised about the amount of sensitive data collected by the National Pupil Database ("NPD") in England (paragraphs 49 - 50)[97] that has been sold to private companies.[98] The NPD has now suspended applications for access pending a review. Each purpose that a child's data is used for must be subject to precautionary measures.

64 **When determining whether the principle of data minimisation has been adhered to, the following metrics might be considered;**

- Context, i.e. different rules for education, social, health, entertainment
- Amount of data, i.e. restrict the amount of data collected by services
- Longevity, i.e. how long the service intends to keep the data
- Sensitivity, i.e. what is the nature of what may be revealed
- Spread, i.e. how far and how quickly does the ISS intend to spread it
- Age, i.e. what age is the child whose data it is
- Purpose, i.e. is the purpose in the best interests of the child
- Specificity, i.e. is it for an anonymised large-scale data set, or is it revealing behaviours and interests of an individual child or identifiable group of children
- An assessment of predictable, but unintended consequences

In an increasingly automated digital environment, the above considerations would offer a guide to 'appropriate' use of children's data.

65 **Children should be given repeated and frequent offers to delete the data they have created, including on logging in, logging out and at predetermined intervals while using an ISS**

66 **Adults should be regularly reminded to set privacy settings on their own devices and services appropriate to the data protection of the youngest user**

THE LANGUAGE AND PRESENTATION OF TERMS AND CONDITIONS AND PRIVACY NOTICES

Meaning

67 Terms and conditions, also known as 'terms of service' and 'T&C's', set out the contract between an online service and the user. They describe the product and services, outline the user's rules of engagement with the service and with other users (also known as 'community guidelines'). Topics covered include; content and intellectual property, information on how a user can modify or terminate their use of services, warranties, disclaimers and liabilities.

68 The privacy notice (also known as 'data or privacy policy') forms part of an online service's terms and conditions. It outlines the information that a user provides when they use the service, the information a service collects,[99] and the information received from third parties. It explains how and why information is used, how it is shared,[100] how long it is stored, and how users can control their information.[101] The privacy notice also sets out the basis or bases upon which the online service is relying to process a user's data[102] and how a user can exercise their rights (including data retention, account deactivation and deletion).

69 Consent to data processing must be given by affirmative action.[103] Under the DPA, children aged 13 or over may consent to ISS processing their personal data (including privacy notices). A parent or guardian must consent on behalf of a child below 13.[104] Non-consent based processing does not require the user's consent to be lawful.[105]

Challenges for children

70 **Children don't read terms and conditions and privacy notices**
It has been estimated that it would take the population of the USA 54 billion hours collectively each year to read the privacy policy of each new website they visit.[106] If adults and/or experts don't read terms and conditions,[107] then the expectation that children do is cynical. Obar and Oeldorf-Hirsch state "the practice of ignoring privacy and terms of service agreements is common knowledge, which points to regulatory failure."[108]

71 **Children don't understand what they are being asked to consent to**
BBC research found that children are signing-up to services (YouTube, Twitter, Snapchat, Google, Instagram, Facebook, Reddit and Apple) with terms and conditions that require a university level education to understand.[109] The Norwegian Consumer Council's report *Deceived by Design* questioned whether a user's consent, given in circumstances where intrusive default settings nudged users towards the least privacy-friendly option, can be said to be explicit, informed and freely given.[110]

72 **Children want to participate**
The reason why children join a service is because they want to use it, often in that exact moment. They see terms and conditions and privacy notices as an unwanted and unnecessary barrier.[111]

73 **Terms and conditions are non-negotiable**
Terms and conditions operate in a "take it or leave it" manner. YouTube, Snapchat, WhatsApp, Skype and many other ISS make joining a service conditional on agreeing wholesale to terms and conditions, including privacy notices.[112] If the price for refusing consent is being locked out of services, many children feel compelled to agree.[113] This raises the question of whether consent can be relied upon as a basis for lawful processing of children's personal data.[114]

74 **Children are developmentally unable to give meaningful consent**
The ICO's *Children and the GDPR Guidance* states that all data controllers must consider the competence of a child to understand the implications of the collection and processing of their personal data. The same guidance also requires data controllers to consider any imbalance in power between the ISS and child when determining whether a child's consent is freely given.[115] Even when children are given an opportunity to grant permission for data to be collected, combined and resold, they are unlikely to fully appreciate the many ways in which this may impact their long-term privacy.[116] In Gillick v West Norfolk

[1984],[117] Mr Justice Woolf stated that "... a child must be capable of making a reasonable assessment of the advantages and disadvantages ... in order for consent to be fairly described as true consent".

If children don't read terms and conditions, don't understand what they mean and are unable to evaluate long-term consequences of agreeing, it is unreasonable for online services to claim that a child has given meaningful consent to process their data.

75 **Terms and conditions presented to children do not reflect their development vulnerabilities**
The understanding that children are vulnerable to commercial pressure, and the expectation that they should not be commercially exploited is set out by the Advertising Standards Authority ("ASA"),[118] the GDPR[119] and the UN Committee on the Rights of the Child[120], among others. ISS' explanations for why user's data is collected does not account for children's credulity, financial situation or development stage.

5Rights recommends

76 **Routine failure by an online service to adhere to its own published rules, including, joining age, community rules, terms and conditions and privacy notices, should be considered a breach of the Code and therefore subject to the full extent of enforcement penalties under GDPR[121]**
Until terms and conditions and privacy notices are upheld by online services, those services should not be entitled to rely on them. The Federal Trade Commission are investigating Facebook for failing to uphold an agreement that stated Facebook would not share users' data without their consent.[122] The Consumer Rights Act 2015 offers a legal precedent for putting published rules on a statutory footing; it requires terms and notices to be fair. Article 62(5) and 62(7) defines that "a term [or notice] is unfair if it causes a significant imbalance in the parties' rights and obligations under the contract to the detriment of the consumer", and will not be binding on the consumer.[123]

The combined effect of rating a service's privacy offer (paragraphs 38 - 39), requiring high privacy settings by default and by design (paragraph 37), and rigorously enforcing the obligation to uphold published terms and conditions, privacy notices and community rules, would be to create a virtuous circle in which a child could instantaneously judge an online service's privacy offer, and the regulator would be able to ensure it was upheld. Thus moving responsibility for safeguarding a child's privacy from the child to the online service and the responsibility for enforcement from the child to the regulator.

Additionally

77 **The limitations of consent as a lawful basis for data processing should be made clear**
Instead, the Commissioner should promote "legitimate interest" (which requires ISS to balance commercial considerations against the best interests of the child) as a more equitable basis upon which to process children's data.

78 **Children must not be expected to police compliance of contracts that they have not read (paragraphs 188 – 189)**

79 **Binary choices should be avoided**
The "take it or leave it" nature of terms and conditions and privacy notices does not allow for meaningful choice. This contributes to an ecosystem that routinely sends the implicit message to children that there are no meaningful choices to be made, thus disempowering them. Standardised privacy regimes that adhere to data minimisation principles (paragraphs 57 - 66) would ensure that terms and conditions are meaningful.

80 **Whilst consent is still in use to collect a child's data, existing ICO guidelines on consent and communicating privacy notices [124] should be included as part of the Code and thereby put on a statutory basis - see Appendix D**

81 **Where written terms and conditions, community rules and data privacy notices are relied upon to establish lawful consent to data processing, they must;**

- **Have a maximum reading age of the youngest person invited to use the service** Language must be appropriate to age and development stage and have a Flesch-Kincaid readability test score

between 60-70.[125] We note that Government's own Digital Service tells online services to write for a 9 year old reading age to ensure that the average person in the UK ,who speaks English as their first language, can understand quickly and easily.[126]

- **Meet the development needs of children under the minimum joining age who use an ISS because the joining age is not enforced**[127]
  For the avoidance of doubt, this is additional to any action taken by the Commissioner against an ISS for failure to uphold its own age restrictions (paragraph 76)
- **Be brought to a child's attention - upfront, in context and on demand**
  Children at different ages may require different placement of privacy information. Younger children are often signed up by parents and then left alone, so upfront privacy is useful. Meanwhile, older children (ages 15 - 17) who are in a developmental stage where risk taking is the norm, may be more likely to adhere to 'in use' messages or on demand. Those aged 10 - 12 would usefully be offered all three repeatedly, since they have the least understanding of consequence, are most likely to take risk and least experienced at using services autonomously. A good practice example is Facebook's pop-up for posting a photo which offers a bright "who can see this?" link that explains that aspect of its privacy terms.[128]

82 **Where it is proven that children using an online service routinely fail to understand terms and conditions and privacy notices, an ISS should be found in breach of the Code and compelled to rewrite them**

83 **The Information Commissioner should explore the potential for joint regulatory action where terms and conditions breach consumer protection law**

84 **The introduction of personalised terms and conditions**
In time 5Rights would like to see the introduction of a single protocol (set of conditions) that meaningfully encompasses all of a child's personal choices about how their data is processed and embodies their individual privacy needs and tolerances. This protocol would be done once, and would then apply wherever they go in the digital environment. It could be changed over time, by the child, to reflect their changing capacity and needs. Such a protocol should be universal, machine readable and industry-wide. Its introduction would reimagine current industry norms that routinely use personalisation for commercial purposes, by putting the same technology in the service, and in the best interests of the child. We note that there is no technological barrier to its introduction, only political and corporate will. [129] Their introduction should not lessen any of the provisions suggested above.

USES OF GEOLOCATION TECHNOLOGY

Meaning

85 Location data is defined in the Privacy and Electronic Communications Regulation ("PECR") 2003 as "any data processed in an electronic communications network indicating the geographical position of the terminal equipment of a user of a public electronic communications service, including data relating to[...](f) the latitude, longitude or altitude of the terminal of equipment; (g) the direction of travel of the user; or (h) the time the location information was recorded."[130]

More colloquially, it is data about where you have been, where you are currently or where you are going.

86 Location data may be made public (by the user, by the ISS or by a third party) and/or it may be collected and used by the ISS without being made public.

87 Some services use geolocation technology directly to perform services, for example; augmented reality games, mapping, transport, food delivery and tracking services. Other services use geolocation for purposes that are not directly related to the users' needs,[131] for example; for profiling, advertising and personalising content.[132]

Challenges for children

88 **Children have to share their location data to access services**[133]
Many services make location-sharing a condition of service, when the functionality required by the child can be provided without knowing the child's location.[134] For example, Snapchat states "when you use our services we may collect information about your location",[135] then states "if you don't agree with [the terms of service], then don't use the Services."[136] If a child posts to Our Stories on Snapchat, their location is shared universally for 24 hours, even when in ghost mode (which is meant to hide a user's location). Snap says, "Story submissions that are set to be viewable by Everyone and any content that you submit to an inherently public service, like Our Story and other crowd-sourced services... may be viewed and shared by the public at large both on and off our services, including through search results, on websites, in apps, and in online and offline broadcasts."

89 **ISS track child users even when they aren't using their services**
For example, Instagram collects geolocation information even when the app is not in active use.[137] That information can be shared across all Facebook Products. Where geolocation settings are adjusted to be more private, they may be switched back on as a result of upgrades.[138]

90 **Children may assume that a device or service is not tracking or sharing their location data because it isn't being published**
Whilst consent to public sharing of a child's location is more frequently (though not always) sought, online services track users (including geotagging and geolocation) for their own purposes by default.[139] Harvard graduate and former Facebook Intern, Aran Khanna says, "because there are no readily visible consequences to sharing location, users are not incentivised to devote attention to what the default of sharing is revealing about them".[140]

91 **It is difficult for users to know whether an online service is using their location**
Google has been found collecting and sharing location data after users disabled their location.[141] And AccuWeather was found to collect geolocation data, despite users not giving permission for them to access it.[142] Apple reminds users when an App is using their location in the background[143] but their promise does not cover Apple's own geolocation settings on the user's Apple device.

92 **Services use location data that is voluntarily given by a child for one purpose, for additional purposes** (paragraph 87)
For example; photographs taken with smart phones or a digital camera often add location and time data as part of the meta-data of the photo, which can then unwittingly be transferred as the image is uploaded. This data may be stripped out when a photo is publicly uploaded, but geotags and the IP address from where a file is uploaded may still remain stored on sites' databases.[144]

93 **Geolocation tracking creates a precise account of the habits and whereabouts of a child**
Including their current location, where they live, the places they like to go and where they might go next.[145]

94 **Location data is used by parents to monitor children**
There has been a recent explosion in services that enable parents to track children's whereabouts without their child's knowledge. For example, the company Footprint allows parents to set up geofences, and be notified when these fences are crossed. Footprints can "activate movement sensors that will notify [a parent] each time [their] loved ones are on the move."[146] EU Kids Online has raised concerns that overprotective parental controls may negatively affect the development of a child.[147]

In 2016, Pew Research Center found that 16% of parents used monitoring tools to track their teenager's location,[148] while an Australian newspaper report suggested it was one in three parents.[149] The Android App store offers over 200 location tracking apps for parents.[150]

95 **Geolocation creates security risks for children from other users and/or security breaches**
For example, adoptive parents report that children have been contacted by birth parents using ISS to find a child's name, location and date of birth.[151] IoT device, CloudPets – a toy that connects children to working parents or grandparents - when hacked, revealed the exact location of the child.[152]

5Rights recommends

96 **Geolocation must be off by default**
Unless a geolocation is service critical (to be determined by the Information Commissioner), it should be off by default. The Code should confirm that it is not in the child's best interests to share their current, past or predicted location for commercial purposes and determine whether there are any circumstances when it may be dangerous, inadvisable or unhelpful for geolocation to be switched off. Where it is unnecessary for the exact location of a child to be communicated to the service provider (for example, navigation apps where a general area rather than specific location can be shared), a child's coordinates and route should be calculated and held within the device and do not need to be collected by the ISS.

Additionally

97 **When a child's location is being tracked, it must be made obvious to the child**
This may be done through the use of an on-screen symbol/light or other indicator. ISS must provide further information about why the child's location is being tracked and with whom their location is being shared. An option not to share must be immediately and easily accessible. In forming the Code, the Commissioner might also consider if the wide range of apps and services used by parents to track children is developmentally appropriate or gives a false sense of security, and if parents have the right to monitor the geolocation of children at all development stages.

98 **Where geolocation is genuinely service critical and in the best interest of the child, the child's location data should expire once that service has been completed (paragraphs 60, 62)**

99 **The Code must establish that it is never service critical or in the best interests to use geolocation to target children or to profile them for commercial purposes**

100 **A child's decision not to allow an online service to track their location should never be a basis for excluding them from a service or deliberately downgrading their experience**

101 **The Industry Code of Practice for the Use of Passive Location Services in relation to children the UK[153] should be put on a statutory footing**
In particular, the parts relating to;

- Parental or guardian consent for a child under 16[154]
- The ability to access all names and telephone numbers of persons authorised to track their mobile telephone[155]
- SMS reminders that others can identify their location[156]
- Any other condition the Commissioner feels is necessary

AUTOMATED AND SEMI-AUTOMATED PROFILING

Meaning

102 Profiling enables aspects of an individual's personality or behaviour, interests and habits to be inferred, determined, analysed and/or predicted.[157] This information can be sorted into multiple categories of user groups and/or provide a detailed picture of an individual user. Vast data sets, and/or the aggregation of one data set with another, combined with the advances in artificial intelligence and machine learning, allow profiles to be constantly adjusted. Profiling both learns from, and is used to determine, user behaviour. It is widely used to evaluate performance at work, economic circumstance, health, personal preferences and attributes, interests, reliability, behaviour, location or movements[158] and is central to targeting marketing content.

103 Automated profiling gathers data and processes it automatically, i.e. without human involvement.[159] Semi-automated profiling is processed with some human involvement, but not enough for that human being to be able to give an explanation for the decision made.[160] The GDPR states that children merit specific protection, particularly where their data is used to create personality or user profiles.[161]

Challenges for children

104 **Children are unaware of the kinds and extent of information that profiling can reveal about them**
For example, emotional states can be predicted from typing patterns on a keyboard, and location data from devices can estimate average income based on neighbourhood and demographic information.[162] While gaming, a player's behaviour can be analysed to create in-depth profiles of their cognitive abilities and personality.[163] Highly sensitive predictions can be inferred from seemingly unimportant or unrelated data,[164] for example, a teenage girl buying unscented lotion, mineral supplements and cotton balls was profiled by Target as being pregnant. Her father found out about the pregnancy (which she had not disclosed) when Target started sending her coupons for baby clothes.[165]

105 **ISS automatically link/share children's data, exponentially increasing the detail of the profile built (paragraph 53)**
ISS share data between their products and services and with other group companies.[166] They share with identified and unidentified third parties.[167] They also combine datasets they collect or receive (e.g. through a device, a connected address book, monitoring use of third party services, website tracking and cookies).[168] Many games collect information about a player's social activities, learning a "tremendous amount of information about the player" from their real-world identity, friends, contacts, likes and dislikes, education, work history and physical appearance.[169]

106 **Profiling can be poor, partial or inaccurate**
Digital profiling based on data (including inference-based data) is used to determine real-world outcomes. Relying principally on profiled data when making important assessments, judgements or inferences about children, may delimit what can be known about them and how they might be treated as a result.[170] Over half a million students and staff are monitored through educational monitoring systems[171] "without oversight or awareness of [the monitoring systems'] accuracy, accountability or otherwise inside black-box decision-making, which is often trusted without openness to human question."[172] If profiling is inaccurate it can lead to mis-identification, or an individual being identified in a way that is not proven.

107 **Consequences of profiling can be discriminatory**
Big data analytics use what has happened in the past to predict the future. The Article 29 Working Group found that profiling perpetuates existing stereotypes and social segregations, restricting users' options and opportunities. It can also lead to inaccurate predictions, denial of services and goods, and unjustified discrimination.[173] Authors of *The Datafied Child* report concluded that there was a "significant risk" that children's opportunities might be narrowed by the assumptions made by algorithmic processes.[174] Assumptions about the prospects and preferences of children based on location, resulted in those from disadvantaged neighbourhoods being offered different opportunities to those living in more privileged areas. This is referred to as "digital redlining".[175]

108 **Consequences of profiling are long lasting**
A child born now is likely to have a footprint from birth,[176] so will have a profile that spans their lifetime over which they have no control.[177] The consequences of this are, as yet, unknown.

109 **It is hard to trace automated determinations back to source**
ISS combine personal information that a child provides when they sign up to a service, with data they collect about how the child uses their services. This information is often packaged and sold to third party advertisers and aggregators, who correlate it with other data sets for further use.[178] This means that it is extremely difficult for any user to trace the reasons for a decision back to the original data source.[179] Unicef states that that there is a "complicated web of legitimate, questionable and illegitimate data acquisition, analysis, brokerage and sale. There is little standard corporate practice".[180]

110 **Data is not neutral – it shapes behaviour, as well as predicting it**
Data is often presented as neutral, but it predicts an outcome based on past actions. Profiling can affect a child's view of their options and/or an outsider's view of the child. For example, in education, learning analytics platforms mine data based on educational tasks and activities, providing automated predictions of future progress that can be used for interventions and pre-emption.[181] It may be used to help a struggling child, but equally it can limit a child's educational pathway.[182] Knowing that information or behaviour will form part of a profile can also lead to self-censoring.

111 **The generation and interpretation of data are influenced by the values, assumptions and biases of those who decide what to collect and how to analyse it**[183]
For example, a study on debiasing word embeddings found that if you put "cmu computer science PhD student" as a query into a search engine, you were more likely to be directed to pages of male students, because the embedding for male names was closer to the "computer science" embedding. This carries implications for children's books, exam questions and news articles.[184] According to the Department for Education, children born in August are 90% more likely to be identified as having a special educational need (SEN) than their older classmates.[185] UCL has found that a SEN diagnosis or label means that teachers are more likely to believe that a child is less able, and as a result, have lower expectations for them, and give them less challenging work.[186]

112 **Children have little control over their profiles, and are unable to seek redress, correction or deletion**
It is extremely difficult to challenge the inferences and predictions that are made by algorithmic calculations.[187] A child may be profiled without course to redress and be unable to have their profile corrected or deleted. Global Privacy Enforcement Network (GPEN) found that only 23% of ISS say how a user could contest a decision made by automated means or request human intervention.[188] It is also unclear how a child might check (or even know to check) whether an incorrect assumption, bias or inference has been made about them.

113 **A child cannot be expected to understand the difference between automated and semi-automated profiling**
If the human intervention in semi-automated profiling is purely administrative and/or confirmatory, it does not offer a high bar of data protection and in the case of children might be better treated on the same, higher bar basis, as automated profiling.

5Rights recommends

114 **Automated or semi-automated profiling that cannot be proven to be in the best interests of a child should be prohibited by the Code**
The Council of Europe suggests that profiling of children should be prohibited by law, save in exceptional circumstances of when it is in the best interests of the child or if there is an overriding public interest.[189] The Council of Europe's Principle 3.5 recommends that "profiling of persons who cannot freely express their consent be forbidden, especially for example, adults with incapacity and children, within the meaning of the United Nations Convention on the Rights of the Child."[190]

115 **Where the Commissioner determines that exceptional circumstances arise and that it is in the best interests of a child to be profiled, a child...**

- **Must be informed about the existence of, and the basis of, automated decision-making processes**[191] **in a clear and accountable manner suitable to the age of the child, by means of a universal icon, symbol light or other marker, as standard (paragraph 97)**
- **Must be able to understand how they have been profiled, and be able to express their point of view about their profile**[192]
  This would require them to be able to (easily) see the attributes, categories of data, and inferences and/or decisions made. It would also require an accessible system of redress or correction that involves human arbitration (paragraph 190).

Additionally

116 **Data used to make automated or semi-automated decisions that have legal effects or similarly significant effects for a child, or where information is obtained through a third party or based on inference rather than volunteered by a child, must be checked by human means for accuracy**[193]

117 **When deciding whether it is in the best interests of a child to profile them, ISS must undertake Child Data Impact Assessments (paragraph 201) to understand the risks and consequences for the child, and ensure that it is not inaccurate or detrimental to a child's wellbeing or life chances**
This should include systems such as those recommended by the ICO, including; algorithmic auditing,

accountability mechanisms for decision making systems, codes of conduct for auditing processes including algorithms involving machine learning, and ethical review boards to assess the potential harms and benefits of profiling.[194]

118 **Data must not be used to infer sensitive information about a child**
Recital 71 forbids the use of data that may infer particularly sensitive information, either alone or through aggregated data being used to profile a child.[195]

TRANSPARENCY OF PAID-FOR CONTENT, SUCH AS PRODUCT PLACEMENT AND MARKETING

Meaning

119 Paid-for content promotes, directly or indirectly, the goods, services or image of a company, organisation or person or specific ideas, social and political campaigns and commercial and non-profit aims in exchange for payment. It does not need to change hands, need not be financial, and may be a mutually beneficial or "reciprocal" agreement.[196] It covers communications that include some marketing elements, even if it is not their main purpose.[197]

120 Direct marketing is "the communication (by whatever means) of advertising or marketing material directed to particular individuals."[198] Targeted direct marketing (also referred to as behavioural marketing) is direct marketing based on knowledge (data) about an individual, where third parties, such as advertising networks, work with websites and advertisers to deliver customised advertising based upon the collection and use of web browsing activity.[199] The vast majority of paid-for content that children see online is targeted.

121 In the digital environment, common types of paid-for content are:

- Search Engine Marketing (sponsored results at the top of search results)
- Pay Per Click (PPC) advertising (banners and pop ups)
- Social marketing (content on social media platforms that promotes a particular product or service)
- Viral marketing (creating content that is shared and spread)
- Influencer marketing (paying famous or popular people to talk about or endorse products and services)
- Product placement and embedded advertising (paying for the deliberate use of, sight of or reference to products and services)
- Content marketing (advertorials, advergames, branded websites and sponsored virtual worlds)
- Retargeting (following a user once they have navigated away from the service, for example, ads that show recently viewed items)
- Affiliate marketing (using affiliates to find and direct new customers to your business)
- Location-based advertising (targeted advertising based on a user's location)

Challenges for children

122 **Children can't spot paid-for content**
Only 22% of 8-11s and 32% 12-15s using search engines, correctly identified that the advertisers had paid for adverts to be at the top. Instead, children thought that they were the best or most popular result.[200] Ofcom found that children find it difficult to point out product placement or native ads (native advertising "goes beyond targeting consumers with ads which are relevant to the editorial they are viewing and seeks to provide content generated by brands which doesn't look out of place in the habitat within which it's being viewed"[201]). In particular they are often unaware that YouTube, Instagram or Snapchat show advertising content. Some children believe that advertising is more trustworthy than the news, as people who purchase a product would be able to spot lies or defects, and that fake news, clickbait, and other paid for content of a campaigning nature, is often accepted uncritically by children of all ages.[202] The increasing use of virtual assistants (for example Alexa and Siri) may further obscure the commercial basis upon which advice is given.

123 **Boundaries between entertainment and advertising content are blurred**
Children in the younger development groups aren't always able to distinguish between real-life situations and fantasy (Appendix A). Ofcom research shows that children are most able to spot adverts that interrupt their viewing or gaming activities.[203] But many situations offer blended or sponsored content with no break. For example; advergames offer an immersive and protracted experience that by their very nature blur boundaries between entertainment and advertising, which is perpetuated by the "mental state of flow that some gamers get into whilst playing."[204]

124 **Children don't understand the relationship between data gathering and paid-for content**
The relationship between a child's search and user history, and the paid for content that they see is opaque. Children may be unaware, for example, that their social media posts are automatically searched and used to determine the paid-for content that they see on their feed[205] or that a company might track how they engage with their services, how they behave elsewhere on the internet, how they use their mobile devices, where they are located or how they use their cursor.[206] In its report, *UK Advertising in a Digital Age*, the House of Lords Communications Committee expressed concern that "many businesses exploit users' data without informed consent."[207] Proctor & Gamble's Chief Brand Officer, Marc Pritchard, described the supply chain of media services from the advertiser to the consumer as "murky at best and fraudulent at worst."[208]

125 **Children are vulnerable to the pressures of advertising**
Marketing practices influence children's behaviour. Prompts to make in-app purchases are found to have a significant impact on children's purchasing behaviour.[209] Susan Linn, from the Campaign for a Commercial Free Childhood, says "Advertising undermines critical thinking and promotes impulsive buying."[210] The EU Commission found that children bought extra features without fully realising that it would cost real money.[211] Children are encouraged to spend money on goods that they have no use for or cannot afford.[212] Children between 10 - 12 were found to be most likely to spend money, or make in-game purchases instead of downloading the free apps.[213] The complex conflicts presented by being offered things they might like but cannot afford, things they might like but may not be suitable for their age or circumstance, things that they would rather not see nor fully understand, create feelings of dissatisfaction and engender the feeling of 'lack' or 'need'.

126 **Adolescent vulnerabilities are exploited**
Teens are extremely attuned to their place in the peer hierarchy, and advertising acts as a kind of 'super peer' in guiding them toward what's cool and what's acceptable.[214] As children enter adolescence and begin forming their identities, they begin to seek out media figures for cues on how to look and act.[215] An influencer can create significant emotional and social pressure to buy that product, even if it is unaffordable or unsuitable. Location-based advertising exploits adolescent vulnerability to impulse buying by radically reducing the time between exposure and consumption.[216]

127 **Behavioural advertising jeopardises a child's right to freedom of thought[217]**
If a child is unaware of the relationship between the monitoring of their online activities and the advertising and marketing content they are exposed to, there is a risk that persuasive techniques might undermine a child's ability to make informed and conscious choices or could be deemed coercive. This also has implications for a child's right to freedom of expression and association.[218]

128 **Data can be used to make wide-ranging inferences**
Mobile phone usage can predict socio-economic status and personality traits; social network profiles can predict impulsivity, depression, life satisfaction, emotional stability, drug use and sexual orientation.[219] A leaked memo from Facebook in 2017 showed that it was able to determine which of its teenage users felt "insecure", "worthless", "stressed", "defeated", "overwhelmed", "anxious", "nervous", "stupid", "silly", "useless" and a "failure".[220] Facebook offered the information to help marketers understand how people "express themselves".[221]

129 **Behavioural marketing can reinforce stereotypes**
Because behavioural marketing offers goods based on previous behaviour, it can have the effect of narrowing available choices. For example, Common Sense Media notes that brands try to establish a

preference for gendered products early in childhood,[222] and the effects of these stereotypes pervade into opportunities they are afforded as adults.[223]

130 **Children are a key market for advertisers**
Unicef notes "Children are of incredible interest to businesses. They are the largest and most powerful consumer group; they are more susceptible to advertising and marketing techniques; and their preferences and behaviours are more open to influence and manipulation. In many ways, they are the ideal audience for the new digital economic paradigm, in which companies possess tremendous amounts of information about individuals' digital behaviour that can be used to shape their online activities."[224] Overall, children and their parents tend to underestimate the commercial interest and transactional value of their personal data.[225]

131 **Advertising is the core business of many ISS that children use[226]**
For example; Facebook and Google earn the vast majority of their income from advertising, and in the UK receive the majority of spending on online advertising.[227] Alphabet reported (2018) that globally, 84% of their total revenue ($32 billion) came from Google's advertising business[228] and in 2017, 98% of Facebook's revenue was generated through advertising (at a total revenue of $39.94 billion).[229] Many games also contain embedded or contextual advertisements.[230] Often services require extra fees to avoid exposure to advertising.[231] Children do not generally have money of their own and therefore are least able to avoid advertising in this way.

5Rights recommends

132 **That the Committee on Advertising Practice ("CAP")'s guidance that requires "enhanced" disclosures[232] for under 12s is extended to all children and incorporated into the Code.** This would ensure that:

- Marketing communications are obviously identifiable to children
- Advertising is "prominent, interruptive and sufficient to identify the marketer and commercial intent"[233]
- Marketing communications make their commercial intent clear for children
- There would be a labelling scheme
- Marketers adapt to children's different cognitive development stages

Additionally

133 **Children's data must not be processed for behavioural advertising purposes**
As children are unlikely to understand the persuasive intent of behavioural marketing, they should not be exposed to behavioural advertising.[234] The Working Party 29 Opinion on Apps on Smart Devices specifies "data controllers should not process children's data for behavioural advertising purposes, neither directly nor indirectly, since this will be outside of the scope of the child's understanding and therefore exceed the boundaries of lawful processing."[235] The Working Group's determination is equally relevant to behavioural advertising on all online services.

134 **The cost and frequency of in-app purchases should be indicated as part of signing-up**
And be taken into account when age-rating games. In all cases, it must be possible to disable in-app purchase offers and still play the game.

135 **Children's data must not be used in a way that might lead to their commercial exploitation**
When determining if exploitation has taken place, both the actions taken to persuade a child to do something for commercial purposes, and the protections offered to prevent their commercial exploitation, should be taken into account.

THE SHARING AND RESALE OF DATA

Meaning

136 Once gathered, data can be shared, rented or sold. Sharing and re-sale of data includes 'in-house' as well as with third parties, such as suppliers, subcontractors, advertisers, marketers, data sale agents, analytics

companies, public institutions, private companies and government. It can be shared in the UK and across international boundaries.

137 When shared, data can be anonymised, pseudonymised or transferred in a way that openly identifies individual users. Specific data can be shared, or it can be shared as part of data sets. It can be shared as raw data or inferred data. Sharing may happen once, or it may be ongoing. The GDPR recognises that the "scale of the collection and sharing of personal data has increased significantly."[236]

138 The sharing and resale of data is the business model of many ISS (paragraphs 149 and 177) but public bodies also hold, share and sell data. In the case of children, data held by public bodies may relate to their health, education, family and status. Individuals, including children, also voluntarily share data.

Challenges for children

139 **Children create a lot of data**

Children create a great deal of data in almost all areas of their lives; education, social, entertainment and communication. Their data is also captured by their network, e.g. in schools, health services, government records, parents and other adults, as well as by the commercial online services with which they interact. The sum total of this information is then often shared and/or sold in ways that they do not know or may not understand, but which might not be in their best interests.

140 **It is easy to lose control of data dissemination**

The technical settings and social pressures to share, set a low bar of distribution of a child's data through their network. For example, via personal networks, e.g. screenshotting, re-tweeting, copy all, chat groups, etc. Less visible and harder to track is the equally prolific dissemination of data by online services for commercial purposes. Companies, search engines, communication tools and IoT devices collect, store and use digital data in vastly different ways that make it virtually impossible to paint a comprehensive picture of data collection practices.[237]

141 **The sharing supply chain is very opaque**

In 2017, GPEN found that 51% of websites fail to mention that they share data at all.[238] Unicef has concluded that "with increasingly autonomous software and hardware, hidden discreetly within the technology that accompanies users wherever they go, users are ever more ignorant of how their devices actually work and the extent of what they are monitoring and sharing."[239] This raises the question whether a child can conceive of, and meaningfully consent to, all the sharing involved; as children's data is passed to third parties who can use it for marketing purposes or to train new systems and artificial intelligence.[240] Irrespective of the basis of lawful processing, what additional responsibilities should the ISS have for sharing children's data than they have for processing it for their own purposes?

142 **It is hard to monitor misuse**

Due to this lack of transparency, it is extremely difficult to trace and challenge data misuse by online services. Additionally, children struggle with interpersonal misuse (bullying, body shaming, etc.). When personal data about a child has been disseminated publicly, they find it hard to retrieve, retract or erase data that they have shared, or which has been shared by others about them within their social network, and very often far beyond.

143 **Consequences of sharing and resale of data can be significant and long-lasting**

Even when a child is given an opportunity to permit data to be shared and resold, they are unlikely to fully appreciate the many ways in which this may impact their long-term privacy[241] and reputation[242] (paragraph 187). In the UK, a YouGov study found that only 31% of employers would not, or do not search for candidates on social media, and one in five employers had turned down a candidate because of their social media profile.[243] Online histories are arguably becoming more valuable than credit histories,[244] creating the spectre of a child being turned away from an opportunity in the future because of inferences or data shared in the past. Data of which they may have no knowledge, and over which they have no agency.

144 **Parents also share children's data**

It is commonplace for parents to share information about their child online, yet most children are not able to scrutinise the information or object to its posting. Parents may not understand their role in compromising their children's privacy far into the future.[245] Nor do parents always understand just how widely what they share is shared, or the ways in which it may be interpreted.

145 **Sharing is a condition of service (paragraphs 68, 88)**

5Rights recommends

146 **In considering if an online service has met the "best interests" of a child when sharing their data, the Commissioner must take into account the 'intention' of the ISS in sharing that child's data**
The introduction of the Code should in itself create an ecosystem in which children's data is more carefully collected and shared, but when determining whether an ISS has complied, the Information Commissioner should consider whether, in sharing a child's data, the ISS has given paramount consideration to the best interests of the child.

For the avoidance of doubt, even if it is in a child's best interest to share data in the course of playing a game or posting a picture, etc. it should not be interpreted as being in their best interests to share that data with third parties or to keep it longer than it is service critical to do so. In particular, data sharing policies must reflect both the spirit and the letter of the six principles of data minimisation,[246] and the right of a child to privacy.

Additionally

147 **A child's consent to data sharing should not be unlimited**
Continuous sharing of data through extensive chains that cannot be traced and for which the online service is not held accountable, is not in the best interests of children. The assumption must be that the only sharing to which a child has agreed is the initial sharing with the online service to the extent that such sharing is service critical.

148 **The following sharing norms should be introduced by the Code;**
For youngest children: (i.e. 0 - 5, 6 - 9)
A closed setting/walled garden environment. No commercial sharing not even within company ecosystems.

For older children: (10 - 12, 13 - 15)
As children get older, they may benefit from features such as exchanging messages, learning to be responsible and knowing what to share safely. These should be designed for minimal public sharing. Commercial data sharing should be predicated on data minimisation principles and should be service critical (paragraphs 57 – 66).

For 16 - 17 year olds:
In this age group, ISS may assume a level of understanding and agency and therefore exercise some discretion over their data sharing, subject to the introduction of other protections set out in the Code.

149 **ISS should be required to create choice architecture and offer tools that might nudge or help children to undertake thoughtful sharing**
For example;

- a screenshot prevention tool (often asked for by children)
- software that limits the time content is available (e.g. Snapchat)
- a "trust pause" where children can stop and think before they automatically click, swipe, or share content - as standard[247]
- awareness campaigns i.e. #nodacompartir (it's not cool to share) in Argentina[248]

150 **ISS should be required to do due diligence on data recipients before sending or sharing a child's data and remain liable for the way that a child's personal data is subsequently used after it has shared or sold it**

5Rights advocates for the creation of an ethical data supply chain. [249] This might, for example, place a requirement on the online service to make enquiries about the intended use of the data, including the efficacy of algorithmic profiling or whether the data processor intends to generate inference-based data about a child. It might also oblige the online service to satisfy itself that the recipient will store the data securely and be able to comply with a request to recall and/or trace what has been shared.

STRATEGIES USED TO ENCOURAGE EXTENDED USER ENGAGEMENT

Meaning

151 Extended use strategies, based on the science of 'persuasive design' (also known as 'behavioural design')[250] are those features that direct, nudge and influence user behaviour for the purposes of extending engagement. Technical strategies (no save button or auto-play) and emotional strategies (designing social obligations and/or anxieties into services), work singly or in concert to summon users to engage with a service and to hold their attention once engaged. Extended use design[251] includes features such as; notifications (buzzes, pings, vibrations), read receipts, auto-suggested content, loading wheels, endless feeds, quantification (the number of Likes, retweets, friends) and obligation (streaks, read receipts).[252]

152 Services that look free to children most often have a business model that is predicated on commoditising personal data or selling users attention to advertisers.[253] The longer a child spends on a service, the more actions they take and the more data is gathered, including data used to direct advertising. Even subscription services (those that accept payment in exchange for services) use persuasive strategies. Extended use, the deployment of extended use strategies and data collection are inextricably linked.

153 The use, presence and power of extended use strategies are disputed by some companies. "Encouraging addictive behaviour does not factor into the process" (Facebook). "We do not employ design techniques to encourage compulsive or addictive behaviour" (Snapchat).[254] These statements conflict with Sean Parker's, co-Founder of Facebook, explanation that "the thought process that went into building these applications, Facebook being the first of them... was all about: how do we consume as much of your time and conscious attention as possible?"[255] They also conflict with the work of Tristan Harris, a one-time Google Ethicist who set up the Center for Humane Technology and has partnered with Common Sense Media to lead campaign, the Truth About Tech.[256]

154 In South Korea, compulsive use of technology among children is formally recognised.[257] In the UK, children are now able to seek treatment via the NHS after video gaming addiction was classified as a medical disorder[258] under the World Health Organisation's International Classification of Diseases (ICD-11, currently in Beta form).[259] In the US, a letter from Apple investors in January 2018 recognised compulsive use as an unacceptable harm,[260] and in June 2018, 5Rights published *Disrupted Childhood: the Cost of Persuasive Design*.[261]

155 Unicef is one of many organisations that recognises extended use as an issue for children: "the aim is to play on the desire for social acceptance and exploit the fear of rejection. While the average user might disengage from the platform minutes or hours later than intended, coming away with little or no benefit, tech companies come away with financial gain from advertisers, plus their users' time, attention and personal data. Adolescents, already experiencing new and complex emotions, might not realise the potential impacts on their privacy or how they spend their time."[262]

Challenges for children

156 **Extended use strategies are habit-forming**

Persuasive design deliberately reinforces digital habits, such as subconsciously reaching for a device, refreshing pages and profiles to check for new content, and locking and unlocking devices. Young people are particularly vulnerable to compulsive use because they are less able to self-regulate and they tend to seek instant rewards (Appendix A). Ofcom's 2017 media report also showed that children choose media activities based upon habit.[263] Routines and habits formed before the age of nine[264] take considerable interventions to change.[265] Netflix CEO, Reed Hastings explained that there is a race for human attention.

Netflix, he says, doesn't compete with other companies. "We actually compete with sleep... And we're winning!"[266]

In a large-scale 2016 survey for JAMA Paediatrics, academics from King's College London found "Bedtime use of media devices doubles risk of poor sleep in children."[267] Specifically, it leads to inadequate sleep quantity, poor sleep quality and excessive daytime sleepiness because bedtime use disturbs sleep patterns of children and stimulates the brain's production of melatonin.[268] Children who don't get enough quality sleep are more likely to have excess body weight, poorer diet quality, and lower physical activity levels.[269]

Attachment to their mobile devices also has notable effects in education. London School of Economics found that student performances in exams was found to significantly increase, post a mobile phone ban. Specifically, it found that among low-income and low-achieving students, smartphone use in the classroom exacerbated existing educational inequalities.[270]

Apple's Chief Design Officer, Jony Ive, in response to investor concerns about the addictive nature of the iPhone on children,[271] characterised "constant use" of the iPhone as "misuse".[272] However, products (including the iPhone) and digital services have defaults that maximise use (paragraph 152). As a result, children find themselves trapped in a few highly compulsive digital environments.[273]

Some companies are taking steps to address extended use, following social pressure to reform. Apple's Worldwide Developers Conference 2018 announced design changes to its iPhone to combat phone addiction and FOMO.[274] Google have also announced "wellbeing" features this year, including a dashboard to show users how much time they spend using apps, combining notifications, and setting limits on use.[275] Yet built-in features that require users to tune their own notifications and to set up alerts are not age-appropriate and create unnecessary barriers for child users. And as WIRED remarked, "Apple says it wants you to have a healthier relationship with your phone, and it'll even give you the tools to do it. But for every feature it showed to wrangle notifications or curb app use, it added more to keep you staring at your screen."[276]

157 **Extended use strategies are baked in to devices and services that children use**
Children spend the majority of their time on a small number of commercial services,[277] all of which have persuasive features. For example; endless newsfeeds (Facebook); auto-play (Netflix, YouTube); streaks (Snapchat); notifications (Talking Tom); quantifying Likes (Instagram, Facebook); quantifying re-tweets (Twitter) and endless scrolling (ASOS). Each creates a cycle of rewards that keep children attached.

158 **Children feel anxious about the amount of time they spend online**
Children report concerns about the amount of time they spend on their smartphones and tablets,[278] saying that they feel unable to switch off, and citing it as a source of stress.[279] They also express resentment when they feel that they have wasted time on platforms and games.[280] Jaron Lanier, the inventor of Virtual Reality, says "customised feeds become optimised to "engage" each user, often with emotionally potent cues, leading to addiction. People don't realise how they are being manipulated... Platforms have proudly reported on experimenting with making people sad, changing voter turnout and reinforcing brand loyalty."[281]

159 **Extended use impacts upon children's wellbeing**
Including; increased risk of depression and anxiety,[282] higher levels of obesity[283] and poorer sleep quality,[284] which in turn diminishes children's ability to concentrate,[285] impacting upon educational outcomes. The need to constantly maintain an extensive online presence creates significant emotional pressure.[286] Persuasive features are deliberately designed to be time-consuming, to maximise interaction for the purposes of data gathering, which means an opportunity cost for children. The time they spend attending to the flow of content and reward, is time that cannot be spent doing other activities, including other more intentional online activities. Childhood is a time of rapid physical, emotional and intellectual development when children should be exposed to a broad set of physical, social, creative and intellectual activities. Being persuaded to engage in a narrow band of digital activities may not be in their best interests.

160 **The use of persuasive design undermines the notion of consent**
If extended use strategies are habit-forming, a child's freedom to freely give or withhold consent is fettered. The Commissioner may wish to consider whether such consent is valid where strategies are routinely deployed. Potentially addictive or harmful substances are taxed and strict regulations are in force to limit children's access to them (paragraph 162). Such interventions might offer precedents that could be applied to the regulations of compulsive technology.

161 **Extended use strategies are not compatible with data minimisation principles**
Extended use strategies are deployed to maximise the amount of time a user spends online, and therefore create the opportunity to maximise data generation and collection. This conflicts with the requirement under the GDPR to limit data processing to that which is "adequate, relevant and limited to what is necessary."[287]

5Rights recommends

162 **The characteristics of persuasive design that make online services compulsive must contribute to an ISS' overall privacy rating. These characteristics should be identified, rated and labelled in a way that is easily identifiable to a child or parent**
Persuasive design strategies are problematic for children because they are hard to spot. Labelling would make it easier to make informed choices about which services to use. It may also help those who are struggling to moderate use. A rating system, based on a universally agreed system, could be reflected as icons and would form part of advice on whether digital products are age-appropriate (paragraph 38). It is noted that classification of energy ratings,[288] carbon emissions,[289] nutritional value[290] and games[291] are all social norms, and that pharmaceuticals, finance and other Use of Service agreements, offer warnings of potential risks, negative effects and safety information.

Additionally

163 **These features should be made age-appropriate in the following ways:**

- Auto-play should be default off, and if changed, switched back to off once a child logs out or navigates away
- Notifications, buzzes, read receipts and all other non-specific alerts should also be off by default. The small category of specific alerts includes diary notices and alarms
- Services should not be allowed to distract a child during school hours or when it is in their best interests to be allowed to sleep undisturbed
- Streak holidays (and temporary absences from streak-type settings) should be built in by default
- Save buttons should always be offered, so that children are not forced to stay online to complete a task
- Default timeout and disengagement opportunities that contribute positively to the mental health and wellbeing of children must be standardised, easily accessible and frequently offered, even if it is not in an online services' commercial interests[292]
- Children should be given regular reminders of how much time they have spent on a service
- The use of children's data should be limited, which would reduce the incentive to deploy extended use strategies
- Persuasive designs features must not be enhanced or reinstated when software is upgraded, and meaningful consent must be sought for any new features
- Persuasive design features should never be directed at younger children (under 13)

164 **The Code should recognise compulsive use of technology as a high risk and should recognise it in all interrelated public policy and act accordingly[293]**
For example, the Commissioner should work with Government (including the Department of Health, Department for Education and DCMS) to define compulsive use as a public health issue and an internet risk for children (paragraph 154) and to provide advice and information accordingly.

165 **Children struggling to manage their use of online services should be supported**
For example:

- ISS should provide in service information and signpost external services that can offer support to children who are worried about compulsive use
- iOS and Android Systems must be required to give access to services (e.g. Apps) that help tackle compulsive use to enable them to be integrated into a child's user experience
- Health-based informatics should be used to prompt positive behaviour;[294] the right to rest, enshrined in Article 31 of the UNCRC, that recognises a child's right to rest and leisure, and to engage in play and recreational activities, must be upheld[295]

166 **Personal, Social and Health Education (PSHE), the Computer Curriculum and Relationships and Sex Education (RSE) must include learning how to identify persuasive design and how it impacts on personal data collection and use**

167 **The ICO might usefully publish best practice guidance on the uses of persuasive design in relation to children** (paragraph 204)
Designing online services in accordance with universal standards on accessibility is now an industry norm.[296] Similar guidance on use of persuasive design features in services accessed by children might lead to a sea change in industry practice.

USER REPORTING AND RESOLUTION PROCESSES AND SYSTEMS

Meaning

168 A reporting and resolution process (RRP) is the mechanism through which users contact online services when they experience problems (for example, when their personal data has been misused, misappropriated, it is inaccurate or the child simply regrets publishing it) that they can't resolve alone and/or need action to be taken. RRP may be located in settings, in FAQs, in the Help section or elsewhere on an ISS. It may be activated via support dashboards, 'chat' windows, by completing online documents or forms, or sending direct messages or emails.

169 They may relate to data of general nature (adverts watched, tracks played); a highly personal nature (photograph, phone number, location); they may include data that may be inaccurate, defamatory or illegal; that may be misappropriated, misused or regrettable; or that may be simply a request for information.

170 RRP's are used for multiple reporting issues, e.g. contact, conduct and content issues, as well as those concerning data and must be designed to cover all these eventualities in relation to children.

Challenges for children

171 **Children under report issues**
For example, only 12% of UK 9-16 year old's who were upset or bothered by an online risk used reporting tools.[297] There are multiple barriers to reporting and children lack the skills, confidence and knowledge in the reporting process.[298] Younger children don't know how to make a report, they don't know what a report is, they don't think reporting will help, and they feel that reporting can result in negative consequences.[299] Older children are more likely to not report because they don't think it will make a difference,[300] they find the processes arduous, and they forget that the reporting tools are available.[301] Adolescents, in particular, may strive to be 'street wise' in the digital neighbourhood, and not feel able to share anxieties.

172 **Having the technical ability to report does not in itself make it likely or probable that a child will make a report or that the report will be successful[302]**
In the House of Lord's *Growing Up With The Internet* report, children reported believing that only the uploader of content could take it down.[303] For children to report, there has to be clear benefits, easy access and the ability to remove content themselves.[304] Despite many ISS having strict community standards, children say that they struggle to get content relating to them removed from the internet.[305]

173 **Children may not want to ask their parents for help**
Younger children are more likely to welcome parental mediation.[306] Older children are more likely to prefer to talk to their peers and to feel that parents are invading their privacy.[307] In many cases, the need of children for both privacy and a swift response is thwarted by not knowing how to get help or what kind of help they need.

174 **RRP is onerous**
RRP mechanisms are not standardised, nor centralised. Online services have resisted calls for universal standards and signposts, but for children they offer security and clarity, much like the Green Cross Code, BBFC age ratings or a red cross on the first aid box. If the data a child is contesting has spread, the current norm is that a child is required to understand and navigate different processes of each service and to make multiple complaints/requests in different formats. Children repeatedly ask for the experience of reporting to be the same or familiar, for the standards to be consistent, the punishments to be the same and to be better informed throughout.[308]

5Rights recommends

175 **The Code introduce mandatory universal reporting standards so that the criteria, systems and likely outcomes are familiar to children**
By which we mean, that the steps a child takes, the information offered, and outcomes of reporting should be similar. By which we do not mean that a site cannot use its own brand or speak in a branded voice. The following aspects of RRP should be standardised:

- Information about reporting must be provided upfront and during use of service in unavoidable text or video
- **Process** - reporting should be intuitive. Many of the individual sites have good systems. For example, YouTube has a reporting dashboard that allows users to see the status of videos they have flagged for review.[309] Examples of best practice should be consolidated and extended to form industry-wide, universal standards that recognise the development needs of children at different ages (paragraph 204)
- **Placement** – it should be obvious how to report
- **Criteria** - must be consistent so that a child can understand the norms of online rules
- **Reporting** - transparent reports on numbers of requests received, response times, steps taken and outcomes. Companies have had many opportunities and failed to uphold voluntary reporting. The Code offers the opportunity to make reporting needs of children mandatory for all ISS
- **Testing** – Robust testing with children in all age groups would ensure that RRP solutions are child-friendly and cover the full gamut of childhood complaints and anxieties, and would enable ISS to determine that their child users have the developmental capacity to access and activate proposed RRP mechanisms

Additionally

176 **Reports by children, or by adults on behalf of a child, should be graded by urgency (from the child's perspective) and each grade should carry an expectation (set out by the Commissioner) of a response time frame**
For example; 'Letting you know', 'Can you get back to me', 'This is important', 'This is urgent'. Each should have its own published time frame. This would allow a child to assess their own situation, which in itself is an educational measure. The ICO should consult with industry before setting appropriate time frames for response and determine penalties for failure to respond. A child's determination of how urgent their request is in addition to, not instead of, appropriate triage systems and must not be used to downgrade their complaint.

177 **RRP tracking should be compulsory for ISS with high reporting levels**
A service that routinely has more than a specified number (to be determined by the Commissioner) of reports from children per week, must introduce a RRP tracking feature that makes clear to the child what is happening to their complaint and when it might be resolved (in the same way that delivery services make it possible for customers to track a delivery, e.g. Amazon, Asos, Deliveroo, Uber).

178 **On rejecting a request from a child to activate their data rights, an ISS must be required to provide reasons and information on how to appeal**[310]
For example, by offering a direct link to the ICO and designated points of contact for relevant organisations and hotlines.

179 **The Code should require ISS to consider and mitigate privacy risks for children using RRPs**
To consider a request made by a child, an online service will need to review and potentially store personal data about the child. The Code could determine how the child's personal data is kept and stored in a way that does not make reporting a data risk.

THE ABILITY TO UNDERSTAND AND ACTIVATE A CHILD'S RIGHT TO ERASURE, RECTIFICATION AND RESTRICTION

Meaning

180 Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences, safeguards concerned and their rights in relation to the processing of personal data.[311] Therefore, children require a higher bar of data protection. They also, by virtue of their development stage, require greater support in accessing their rights.

181 Like adult data subjects, a child may complain to the ICO or bring legal proceedings against a controller or processor should they suspect non-compliance. However, data protection rights are complex, and for most adults and all children, they are a new concept. To be effective, children need a way to activate their data protection rights. A right that cannot be understood or enacted is not properly given.

Challenges for children

182 **Children's rights are poorly applied**
Children have many of the same data protection rights as adults, as well as data rights that apply to them only. However, they have other rights that impact on data protection (most notably those under the UNCRC) that are routinely ignored. The Committee on the Rights of the Child notes that, in all circumstances, generic policies that fail to recognise children separately, i.e. those that consider children and young people often fail to address adolescents "are inadequate to guarantee the realization of their rights. The costs of inaction and failure are high... [and] have profound implications, not only for their individual optimum development, but also for present and future social and economic development".[312] **This observation is central to this aspect of the Code, and the Code overall.**

183 **Children do not have the education or capacity to understand their data rights**
43% of teenagers have posted information online they later regretted,[313] yet most children are not taught about data rights; 58% children mistakenly believe that online data can easily be removed if they no longer wish to share it with other people[314] and that once deleted from view, it does not form part of their digital identity. They have little idea about profiling or how data spreads (paragraphs 104 - 105). As such, children are unable and/or unlikely to exercise control easily (such as accessing, retrieving and deleting their data).[315]

184 **Children in the age groups 3 - 5 years and 6 - 9 years cannot be expected to understand data rights in any meaningful way**
Children ages 10 – 12 and 13 - 15 can be expected to understand the concept of retraction and rectification if taught well, but they cannot be expected to activate these rights without support, or in a context where statutory education does not fully explore these issues. Even children aged 16 - 17, who may well have both a conceptual and practical understanding, require signposts, simplicity and to grow up in a digital environment that encourages reporting (paragraph 175).

185 **Adults don't understand data rights so are poorly placed to help children**
Even the expert Parliamentarians who led the debate on the Data Protection Bill acknowledged that data law is not easy to understand. Lord Ashton of Hyde, the Parliamentary Under-Secretary of State, DCMS said "I find it quite complicated".[316] While Lord Stevenson of Balmacara stated it was a "complicated

area"[317] and Lord Clement-Jones said that the Bill had "already had a befuddling influence".[318] ICO research found that only 10% of adults say they have a good understanding of how their personal data is used.[319] Data protection is a specialist area.

186 **Children cannot be expected to identify one form of rights abuse from another**
Data breaches, wrongful use of personal data, illegal uses of data, illegal content, reputational damage, defamation, direct marketing, contraventions of the Age-Appropriate Design Code (once introduced) sit alongside other experiences that may seem similar to children or indeed overlap, such as; bullying, unwanted photo tagging, fake news, phishing, scamming, grooming, hate speech... an exhausting but non-exhaustive list of what children experience. In this context, the activation of data rights takes on an auditing and signposting role, as well as securing the mechanisms and support to activate a child's right.

187 **Reputational management**
The online environment has transformed the concept of managing reputation by dramatically increasing the scale, scope and reach of information. An average childhood is now a public experience. Inaccurate or revealing data is duplicated and effectively stored in perpetuity. As children publish personal information about themselves and others at progressively greater rates, antisocial attacks on reputation have proliferated.[320] At a time of great vulnerability and emphasis on validation by peers, a child's data rights, as they affect their enduring online identity, are of paramount importance to their identity, safety and wellbeing.

188 **The onus is on an individual child to activate their rights**
Children under report, systems are unclear, they do not have the development capacity and companies do not collect adequate reporting data, which makes the likelihood of a child bringing a claim vanishingly low (paragraphs 171 - 174). This protects the poor performance of online services handling children's data, since they are unlikely to be held to account.

189 **Children are being asked to generate their own data complaints**
Article 80(1) of the GDPR allows children to mandate certain organisations to bring a claim on their behalf.[321] However, this requires a child to initiate the complaint and be a named complainant, in effect leaving children to police the law. 5Rights regrets the UK's decision not to enact Article 80(2) but rather to undertake a review that will not report until the end of 2020.

5Rights recommends

190 **ISS should be compelled to enact basic rights by design (such as the right to retract, rectify, erase, access, obtain, modify, reuse personal data) by offering simple, standardised tools within services that children can recognise and readily access**
For example, click-through mechanisms for deletion, retraction or correction for anything they themselves have put up, and in cases where community rules have been breached. When asked, children repeatedly say that they want the right to have content taken down.[322]

Additionally

191 **The Code should create a rebuttable assumption in favour of accepting a child's request to activate their rights. In the balance between free speech and privacy, the privacy of a child under 18 should be given pre-eminence**

192 **That government adopt 80(2) on behalf of child data subjects**

193 **ISS that share a child's data be responsible for tracing that data, and ensuring that the child's request to enact their rights is passed to all those who have processed it**
It is an arduous and age-inappropriate task for a child to have to make repeated requests to different ISS.

194 **If a child has not been asked to prove their age to join a service, they shouldn't be required to prove it to benefit from the specific protection of the Code to which all children are entitled when activating his or her data rights**

195 **No child should have to pay to activate their data rights**

Complaint mechanisms should always be free to access. Children wishing to pursue their complaint further should have access to free legal services and other appropriate assistance.

THE ABILITY TO ACCESS ADVICE FROM INDEPENDENT, SPECIALIST ADVOCATES ON ALL DATA RIGHTS

Meaning

196 The implications of misuse of data can be profound for children (paragraphs 127, 143, 159, 187). Children, parents, teachers and those with special duties for children rarely have knowledge about data rights. To activate their rights, children require access to specialist advice and support from independent advocates.

Challenges for children

197 **Children, parents and trusted adults are unlikely to know what advice to give or action to take**

198 **The most easily accessible advice is that offered by companies with whom children are engaged**
If the advice is written and delivered by the services that they are engaged with, it creates the perception and possibility that advice is partisan. Children require access to independent, specialist help to understand and enact their data rights.

5Rights recommends

199 **The ICO should, by way of the Code, make data privacy a more mainstream preoccupation for those with responsibility for children**
Specifically, government - particularly DCMS, Department of Health, Ministry of Justice, Department for Education and Home Office - must make sure that they, and those professionals that they work with, have a good understanding of children's data rights and that they form part of professional qualifications and training for those roles (paragraph 206).

Additionally

200 **The Code should refer to other relevant laws that may impact on children's data rights.**
For example; The Consumer Rights Act 2015 requires terms and notices to be fair. Article 62(5) and 62(7) defines that "a term [or notice] is unfair if it causes a significant imbalance in the parties' rights and obligations under the contract to the detriment of the consumer" and will not be binding on the consumer.[323]

ANY OTHER ASPECT OF DESIGN

Q5E. About any additional areas, not included in the list above that you think should be the subject of a design standard.

The following points would enhance the effectiveness of the Code by addressing overarching issues.

5Rights recommends

201 **Childhood Data Impact Assessments as standard for all existing services and products, and new services and products prior to launch**
The GDPR requires Data Protection Impact Assessments for all processing that is likely to result in a high risk to the rights and freedoms of users,[324] and the ICO provides guidance on the circumstances where DPIA are required.[325] Building on this, 5Rights recommends requiring online services to carry out Child Data Impact Assessment (CDIA) for all online services likely to be accessed by a child. The CDIA would address the specific needs and higher standards to which children are entitled, and place the requirement to carry out such assessments on a statutory footing.

The "move fast and break things"[326] and "fail furiously"[327] culture of the technology industry does not hold the best interests of the child as their primary consideration. Introducing Child Impact Data Assessments before services and products are rolled out would circumvent some of the most obvious data risks. The

Commissioner might consider using the Responsible Innovation Framework as defined by the Engineering and Physical Sciences Research Council[328]. A part of the Child Impact Data Assessment should include ongoing and open engagement with a wide user base, including experts, key stakeholders and children on the interpretation and application of privacy standards and their effectiveness or appropriateness.

202 **A proactive approach: via certification of ISS data provisions**
Rather than regulators only acting once something goes wrong, the ICO might consider the role of certification systems. For example, the World Economic Forum recommends encouraging regulators to certify that algorithms are fit for purpose before they are used.[329] A certification, or self-certification system, specifically tailored to the needs of children as set out by the Code, would increase compliance levels and support a swifter and more streamlined enforcement regime.

203 **Information provision: harness the Commissioner's duty to promote public awareness for the benefit of children**
Article 57(1)(b) of the GDPR places a duty on the Commissioner to "promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing", giving specific attention to "activities addressed specifically to children".[330] The Government's review of PSHE and the Internet Safety Strategy's commitment to digital literacy[331] mean that there is an opportunity for the National Curriculum to teach about privacy in a way that aligns with children's developmental capacity. For example, young children (KS2) should receive digital skills and competencies[332] education before they need to adjust privacy settings.[333] The ethical design and use of AI could also form part of the curriculum as the ability to "navigate an AI-driven world will be essential".[334]

204 **Audit & collate codes: there are a plethora of codes, often narrow and/or unobserved. Their provisions should be incorporated within the Code and therefore put on a statutory basis**
The Age-Appropriate Design Code presents a unique opportunity to work with industry to encapsulate existing best practice across all the different aspects of design and to 'level up' and put self-regulatory codes on a statutory footing within the Code. A single, clear, robust, well-thought-out set of design, technical and corporate behaviours would become a new norm. This would help the whole tech sector to flourish and confirm the UK as a world market leader. It would also reward those already applying best practice, since they would meet the requirement of the Code quicker. SMEs, start-ups and individual designers, as well as training and education, would also benefit from a single set of best practice standards to design to.

205 **Educative function: Online services often use education of children as a way of avoiding responsibility. Systemic redesign of services that enhance children's rights in the digital environment could usefully play an educative function in demonstrating privacy and safety features to children**
As part of an online services' educative function, they should optimise interactions through features and functionality that target, signpost, prompt and support user empowerment as part of the in-service experience. This should be implemented across all aspects of design.

206 **Training for frontline professionals: Ensure frontline professionals (for example, teachers, social workers, health and legal professionals) have appropriate training and a broad understanding of the full range of opportunities and risks in the digital environment, including all aspects of design covered by the Code**
Include training as part of degree accreditation and professional standards.[335]

207 **Robust enforcement: The Code requires a continued commitment from Government to enforcement**
Unless there is a meaningful likelihood of enforcement, the ISS are not incentivised to implement the Code in ways that are robust and effective. The ICO needs sufficient expertise and resources, and, given the huge wealth of some ISS, the backing from HM Treasury to fund enforcement. We note and welcome the ICO's increased budget and the commitment Government has shown to resource its vital work.

Q6. If you would be interested in contributing to future solutions focused work in developing the content of the Code please provide the following information. The Commissioner is particularly interested in hearing from bodies representing the views of children or parents, child development experts and trade associations representing providers of online services likely to be accessed by children, in this respect.

Brief summary of what you think you could offer:

208 5Rights, its network of experts and its children's Commissioners would welcome the opportunity to engage on all aspects of the Code.

FURTHER VIEWS AND EVIDENCE

Q7. Please provide any other views or evidence you have that you consider to be relevant to this call for evidence.

209 The opportunity afforded by the Code is to design a digital environment fit for children and childhood and to build trust in ISS. 5Rights is committed to the positive uses of technology that empower children to become active and knowledgeable participants in the digital environment.

210 There are however, challenges. not least the lack of a common understanding of what data is, and why it is so powerful in a child's life and that technical solutions do not reside solely with industry but reside increasingly within academia, NGO's, and a growing tech for good sector. We invite industry to share their creativity and expertise with civil society.

211 Whilst help from industry would be welcome, the Commissioner should be prepared to create a robust Code on behalf of children irrespective of industry's appetite to change current commercially-driven data practices.

September 2018

APPENDICES

APPENDIX A - KEY TERMS AND CONCEPTS

Age Appropriate Design Code

212 The Age Appropriate Design Code is a requirement of the DPA, which provides statutory guidance on the design standards that providers of online services, which process personal data and are likely to be accessed by children, must meet.

Data processing

213 Processing is how data is gathered, arranged, stored, used or shared. It is any operation, or set of operations, performed on personal data, or on sets of personal data, by any means. Data processing includes, but is not limited to; collection, recording, organising, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[336]

Data Protection

214 Data gathering provides an indelible and highly personal imprint of the person using the services. It both captures and determines behaviour, and as such, it is a very powerful tool that can be exploited for commercial, social and political purposes.

Data Protection Act 2018

215 The DPA contains the UK's data protection laws, in recognition that "an ever increasing amount of data is being processed".[337] Data protection law sets out the obligation upon all online services to ensure that the personal information of those using their services is processed fairly and securely. It received Royal Assent on 23 May 2018.

EU General Data Protection Regulation

216 The GDPR harmonises data protection rules for all companies operating in the EU and regulates the processing of individual's data. It came into force on 25 May 2018.

Information Society Services (ISS)

217 The DPA states that the obligation to comply with the Code applies to Information Society Services, more commonly understood and referred to as online services. The ICO's definition of an ISS includes websites, apps, search engines, online marketplaces and online content services, such as on-demand music, gaming and video services and downloads.[338] We use the terms ISS and online services interchangeably.

Information Commissioner's Office

218 The ICO is responsible for drafting the Age Appropriate Design Code, and for its enforcement.

Personal Data

219 Personal data is information relating to an identified or identifiable person. The person may be identified directly or indirectly. It is difficult to truly anonymise data. Data that might be re-identified and attached to an individual is referred to as pseudonymised data, and still falls within the definition of personal data.[339] This means that the majority of interactions between a child and an ISS result in the creation of personal data.

220 The word data may seem impersonal. However, a child's personal data includes the following information;

Name	Age	Address	Email address
Home address	Photographs	Phone number	Weight at birth
Voice messages	Personal appearance	Exam results	Purchase history

Financial status	Ethnicity	Gender	Medical history
Socio-economic status	Political beliefs	Search history	Sexual orientation
Height	Magazines read	Beliefs	Sleep patterns
Predicted location	Friendship groups	Preferred snacks	Food preferences
Sexual history	School	Hobbies	Languages spoken
Favourite box sets	Country of origin	Social media profiles	Call logs
Allergies	Current location	Number of siblings	Value of family home
Gaming habits	Dietary requirements	Weight	Typical daily schedule
Clothes size	Fitness levels	Emotional state	Intelligence levels
Hair colour	Favourite vloggers	Shoe size	Favourite football team
Location of school	IP address	Openness to advertising	
Preferred fashion brands		In-app purchasing habits	
Preferred music genres and artists		Ability to afford products	
Distinguishing physical markings		School behaviour record	
SMS messages sent and received		Passport number and travel history	
Number of smart devices owned		Amount of make-up bought	
Number of followers on social media platforms		Amount of time spent on social media, gaming or tubing	
Propensity to make impulse purchases			

It is now possible to collect, amalgamate, mine, store and retrieve personal data at a previously unimaginable scale and speed. Information about a child held by online services can go beyond what any friend or family member is likely to know. Perhaps even beyond what a child knows about themselves.

Services "likely to be accessed by children"

221 The Code applies to ISS "likely to be accessed by children".[340] It is therefore not limited to those services that are aimed at children. Rather, it includes the full range of commercial and non-commercial ISS that children are likely to use, or that are ***likely to be accessing*** children's data. We offer examples from a broad and varied set of ISS to illustrate current industry norms and/or point to best practice. However, as outlined in the Government's Internet Safety Strategy Response,[341] most children spend the much of their time using a small group of ISS. Our examples reflect this concentration.

"Specific Protection"

222 Children (under 18s) are often described as digital natives, but this term hides the fact that while they have been swift to adopt digital services, most children remain low on the ladder of digital opportunities.[342] Knowing how to use a handful of online services does not translate to creative or knowledgeable use of the digital environment, nor to an understanding of its purposes, structures and impacts.

223 Children represent 1/3rd of all users online, 1/5th in the UK.[343] They share many of the same rights as adult users but, by virtue of the vulnerabilities associated with their age and development stage, they have additional needs and rights. The Age-Appropriate Design Code will set out in law a data regime that reflects and respects the needs and rights of children, and in doing so, will embody the assertion of the General Data Protection Regulations ("GDPR") that states that "children merit specific protection".[344]

APPENDIX B - CHILDHOOD DEVELOPMENT MILESTONES

224 The following observations taken from MindEd,[345] Piaget, UKCCIS, Unicef, Children's Development Institute, American Academy of Paediatrics and the International Association for Child and Adolescent Psychiatry and Allied Professions[346] give an overview of development capacity in the age ranges set out by the Information Commissioner.

Note: this is a synthesis of multiple dimensions of childhood development including social, language, moral, cognitive and emotional development. It is illustrative rather than exhaustive

Aged 3-5: Children are generally trusting and mostly self-involved

- Children observe and imitate behaviour
- Behaviour is influenced by reward and punishment
- Tendency towards illogical, magical thinking
- Can represent their experiences in speech, gesture and play
- Begin to understand empathy through personal relationships
- Tend to believe what they see
- Cannot use logic to transform, combine or separate ideas
- Play requires a constant flow of language that reinforces link between language and concrete reality
- Egocentric: assume that others perceive, think and feel the same way

Aged 6-9: Children start looking beyond the self to the social world, but have developed few critical skills

- Child's sense of right and wrong is determined by the amount of damage that has been done
- Attention span increases, e.g. a six year old can focus on a task for 15 minutes, while a nine year old can focus on a task for an hour
- Generally trusting of adult authority
- Thinking becomes more logical and rational
- Recognise others' perspectives, but have difficulty with abstract concepts or thinking ahead
- Habit-forming behaviour develops

Aged 10-12: Children start experimenting and risk-taking, and explore beyond family

- Increased independence
- Become relatively less competent at social communication
- Develop more questioning attitude towards authority
- Wide range of complex emotions, relating to social life, including guilt, shame, pride
- Only able to consider what they observe against a backdrop of what is possible
- Are likely to take risks
- Change aspects of themselves to fit in and be accepted by peers, who play an increasingly central role in decision making

Aged 13-15: Children experience polarised emotions, tend towards short-term thinking, and peer approval is paramount

- Complete increasingly complex tasks
- Are likely to take risks
- Look increasingly to peer group to determine features of identity and wellbeing
- Develop attitude towards authority
- Tendency to fierce intensity of high and low emotional experiences
- Boys more likely to display externalising behaviours, including violence, aggression and destructiveness; girls more likely to show internalising behaviours, including depression, withdrawal, eating disorders, self-harm
- While capable of adult-like abstract and logical thought, can struggle to make considered decisions and/or plan for the consequences of their behaviour
- Become relatively slower at tasks that require reasoning skills compared to their speed of responding emotionally

Aged 16-17: Children are preparing for adulthood, exhibiting a broad range of maturities and immaturities within this age bracket

- Able to examine thought processes and engage in abstract thoughts, including future projections
- Use and understand abstract and hypothetical thinking, such as interpersonal relationships, politics, philosophy, religion, morality
- Think in a more strategic manner and can plan more effectively
- Become self-aware and self-reflective. Increasing competence in managing emotions
- Increased independence and self-reliance
- Personal identity, future, skills and talents evolving
- Brain still maturing rapidly
- Emotional and behavioural development continues to inform identity development into early adulthood

APPENDIX C - DATA ROUTINELY GATHERED BY POPULAR SERVICES

The box below shows just some of the data collected by four popular ISS routinely used by children which are indicative of industry norms.

Data Collected by Facebook Products, Amazon, Musical.ly and Roblox

Facebook Products:

- The content, communications and other information a child tells them when they set up their account, create or share content
- The pages they are connected to and view, the features they use, the actions they take, the people they interact with and how long they spend on each activity
- What device the child uses, what browser and network, and their IP address
- Details about what they post or Like
- Anything anyone else shares about the child or tags them in
- The child's address book, if it's synced to Facebook
- The child's telephone call log or SMS log history, if it's synced to Facebook
- The child's photos (if their phone is synced to Facebook and they have approved those settings)
- The child's debit card details, billing delivery, contact details and what they've bought, if they make any financial transaction including buying a game or making a donation on Facebook
- The battery and signal strength on the child's device
- The child's location through the device that they use
- Which devices the child has used to log into Facebook
- Information from advertisers, app developers and publishers who provide information about activities off Facebook, including how the child uses the services (e.g. what games they play or what purchases they make)
- Information collected from cookies on a child's device

Note: Facebook is nominally available only to those 13 and over, but large numbers of children under 13 use the site. A CBBC study in 2016 found that, of the 78% of under 13s using at least one social media network, Facebook was the most popular; 49% claiming to be users.

Amazon:

- Product or services searches
- Uploaded contacts, including the email addresses of friends and other people
- Location of device or computer
- Information and documents regarding identity
- Device log files and Wi-Fi credentials
- Uniform Resource Locators ("URL") clickstream to, through and from Amazon's website (including the date and time), cookie number, products and content viewed or searched for, length of visits to certain pages, page interaction information (such as scrolling, clicks and mouse-overs)
- Information about internet-connected devices and services
- Credit history information from credit bureaus
- File name, dates, times and location of uploaded images and files
- Content interaction information, such as content downloads, streams and playback details including duration and number of streams and downloads, network details, including information about a user's service provider

Note: Amazon clearly states that their Services are only for children with the "involvement" of a parent or guardian. Nonetheless, Amazon sites were the 6th most accessed site by children aged 6-14 from desktop and laptop computers (May 2017) and 24% of 12-15-year olds watch Amazon Prime.

Musical.ly:
Musical.ly collects; browsing records, behavioural information, including engagement scores (Likes, comments, repeated views), information about linking contact or subscriber information with activity across Services (by linking activity on the Musical.ly app across all devices using email or social media log-in details), photographs, and personal data in connection with videos that are uploaded. This is shared with;

- business partners
- advertisers and advertising networks
- suppliers and subcontractors
- analytics and search engine providers
- Joining age 13+

Roblox

- Partners with third party advertising companies to use cookies, beacons, tags, tracking pixels and scripts and other tracking technologies to collect data such as IP address, device ID, and other information about a user's computer or device, as well as internet and online usage information and information about certain activities on the service, including purchases and in-game information
- Provides information to third party advertising companies, including information about a user's visits to the service and other websites, referred to as "behaviorally-targeted" or "re-targeted advertisements"
- Shares anonymised, aggregated, automatically-collected, or otherwise non-personal data with third parties for advertisements and promotions
- Processes location information for services such as targeted or geo-based advertising

APPENDIX D - ICO GUIDELINES

On children's consent to processing personal data:

- Only children aged 13 or over are able to provide their own consent; when under 13, parental consent is required
- ISS should take reasonable efforts to ensure that anyone who provides consent is over 13
- A child must understand what they are consenting to, otherwise the consent is not 'informed' and therefore invalid
- Children may give their consent, unless it is evident that they are acting against their own best interests
- Consent must be freely given; any imbalance in power should be taken into account
- The competence of a child must be considered, and whether they understand the implications of the collection and processing of their personal data
- The age of a child and the complexity of what a service expects them to understand should be taken into account when assessing the competence of a child to consent

On communicating the ISS' use of a child's personal data, privacy notices must:

- Be clear and accessible, and written in concise and plain, age-appropriate language
- Provide children with transparent and clear information, which explains who a service is and how their data will be processed
- Explain to children why a service requires personal data and what they will do with it in a way that they can understand
- Explain the risks of processing data, and how a service intends to safeguard against them, in a child friendly way, so that children (and their parents) understand the implications of sharing information
- Tell children the rights they have over their personal data
- Educate children about the need to protect their personal data
- Distinguish between addressing a 10 year old child and a 16 year old child, and consider providing different versions of privacy notices if an ISS audience covers a broad age range
- Provide child-friendly and adult-friendly versions of privacy notices
- Present privacy notices in a way that is appealing to a young audience, using child-friendly diagrams, cartoons, graphics and videos, dashboard, layered and just in time notices, icons and symbols

ENDNOTES

[1] Department for Education's National Curriculum is divided into: 3-5 (foundation years), 5-7 (infant, KS1), 7-11 (junior, KS2), 11-14 (lower secondary, KS3), 14-16 (upper secondary, KS4), 16-18 (sixth form, KS5)

[2] At 10, children become criminally responsible in England and Wales, however children between 10 and 17 are tried in youth courts and given different (less harsh) sentences. Age of Criminal Responsibility, HM Government.

[3] Section 49 of the Children and Young Persons Act 1933 creates an automatic ban on reporting anything that will reveal the identity of any child involved in proceedings, whether as a defendant, witness or victim. Reporting Restrictions: Children and Young People as Victims, Witnesses and Defendants, Crown Prosecution Service

[4] BBFC Guidelines

[5] Section 123, Data Protection Act 2018

[6] Reporting status for the United Kingdom of Great Britain and Northern Ireland, United Nations Human Rights Office of the High Commissioner

[7] Paragraph 1 "affirms that the same rights that people have offline must also be protected online", United Nations Human Rights Council Resolution A/HRC/70/L.13 on the Promotion, Protection and Enjoyment of Human Rights on the Internet, June 2012

[8] United Nations Convention on the Rights of a Child, 1990

[9] Paragraphs 12, 38, General Comment 14 (2013) on the Right of the Child to Have His or Her Best Interests Taken as a Primary Consideration, CRC/C/GC/14, Committee on the Rights of the Children, 29 May 2013

[10] Paragraph 1, General Comment No. 20 (2016) on the implementation of the Rights of the Child During Adolescence, CRC/C/GC/20, Committee on the Rights of the Child, 6 December 2016

[11] Paragraph 3, General Comment No. 20 (2016) on the implementation of the Rights of the Child During Adolescence, CRC/C/GC/20, Committee on the Rights of the Child, 6 December 2016

[12] United Nations Convention on the Rights of the Child, 1990

[13] Preamble and paragraph 5(g), The Right to Privacy in the Digital Age, Human Rights Council Resolution, A/HRC/34/L.7/Rev.1, United Nations, New York, 2017

[14] A team of Microsoft researchers found that more than 95% of users had kept their settings in the exact configuration that the programme was installed in, as users assume that "Microsoft must know what they are doing" and would have features turned on or off by default, for a reason. The experiment also found that programmers and designers "almost always" changed their settings, some changing as much as 80% of the options in the programme. Do Users Change Their Settings? J. Spool, User Interface Engineering, 14 September 2011

[15] Figure 24, p. 68, Children's Online Activities, Risks and Safety: a Literature Review by the UKCCIS Evidence Group, London School of Economics and Political Science, 2017

[16] Figure 23, p 67, Children's Online Activities, Risks and Safety: a Literature Review by the UKCCIS Evidence Group, London School of Economics and Political Science, 2017

[17] Deceived by Design, Forbrukerradet, 27 June 2018

[18] Transcript of Mark Zuckerberg's Senate Hearing, Bloomberg Government, The Washington Post, 11 April 2018

[19] The experiment by Microsoft researchers found that less than 5% of users who were surveyed had changed any settings at all. Do Users Change Their Settings? J. Spool, User Interface Engineering, 14 September 2011

[20] "We tell the students that their geolocations go on every time they have an update on the Apple phone devices, which a lot of students tend to have these days, and that it turns the geotagging or the geolocations back on" Question 54, Mary McHale, Examination of Witnesses, Evidence Session No. 4, 18 October 2016

[21] From RSA: In Times of Distrust, Innovation and Collaboration Will Be Key, A. Carson, IAPP, 25 February 2014

[22] P. 71, Children in a Digital World, Unicef, December 2017

[23] Pp. 21-22, The Internet on our Own Terms: How Children and Young People Deliberated About Their Digital Rights, S. Coleman, K Pothong, E. Perez Vallejos, A. Koene, 5Rights, January 2017

[24] P. 9, Children's Media Lives: Year 2 Findings, Ofcom, 27 January 2016

[25] Only 10% 12-15s have amended their settings to use a web browser in private mode (Figure 24), and 18% have changed their settings so that fewer people can view their profile on social media (Figure 23). Pp. 67-68, Children's Online Activities, Risks and Safety: A Literature Review by the UKCCIS Evidence Group, London School of Economics and Political Science, 2017

[26] P. 40, Children's Media Lives: Year 2 Findings, Ofcom, 27 January 2016

[27] Facebook's Data Policy states that they "collect contact information if [a user] choose to upload, sync or import it from a device (such as an address book, or call log or SMS log history)" Also: Facebook Scraped Call, Text Message Data for Years from Android Phones, ARS Technica, 24 March 2018

[28] Games can capture behavioral data which is used for targeted advertising and to predict personalities and gamer's economic proclivities. P. 12, Press Start to Track, J Newman, J. Jerome, C. Hazard, American Intellectual Property Law Association Quarterly Journal, 2014

[29] Pp 22-25, The Internet on our Own Terms: How Children and Young People Deliberated About Their Digital Rights, S Coleman, K Pothong, E. Perez Vallejos, A. Koene, 5Rights, January 2017

[30] It can determine educational outcomes, life chances and opportunities, and impact on their ability to access services Pp 2, 7, 8, 12, The Datafied Child: The Dataveillance of Children and the Implications on their Rights, D Lupton, B Williamson, New Media & Society, 19(5), 23 January 2017

[31] "Children are a particularly vulnerable group of users, because they often lack the awareness and the capacity to foresee possible consequences". P. 34, The Protection of Children Online, OECD, 2012

[32] The Maturing Adolescent Brain, A. Morelli, 17 November 2010

[33] P. 8, The Datafied Child: The Dataveillance of Children and the Implications on their Rights, D Lupton, B. Williamson, New Media & Society, 19(5), 23 January 2017

[34] 51% of aged 12 years old and under have a social media account. P. 102, Children and Parents: Media Use and Attitudes Report, Ofcom, 29 November 2017

[35] "By default, anyone can view your profile and posts on Instagram". Controlling Your Visibility, Instagram "Your Tweets are public by default: anyone can view and interact with your Tweets... whether or not they have a Twitter account". About Public and Protected Tweets, Twitter

[36] P. 68, Children's Online Activities, Risks and Safety – A Literature Review by the UKCCIS Evidence Group, London School of Economics and Political Science, 2017

[37] Deceived by Design, Forbrukerradet, 27 June 2018

[38] Paris Brown: Kent Youth PCC Resigns After Twitter Row, BBC News, 9 April 2013

[39] Revealed: What the SNP Candidate for Paisley and Renfrewshire South Thinks About Football, Daily Record, 6 February 2015; We Enjoyed Reading Mhairi Black's NSFW Tweets as a Teenager, The Independent, 2015

[40] Paragraph 19, Horizon Digital Economy Research – Written Evidence, (CHI0032), 26 August 2016

[41] The Internet of Toys, G. Mascheroni, Parenting for a Digital Future, London School of Economics, 27 January 2017

[42] #WatchOut, ForbrukerRadet, October 2017

[43] Strava's Data Lets Anyone See the Names (and Heart Rates) of People Exercising on Military Bases, WIRED, 30 January 2018

[44] Which? Report Calls for Staggering Level of Smart Home Security, A. Laughlin, Which? 1 June 2018

[45] Press Start to Track? J. Newman, J. Jerome, C. Hazard, American Intellectual Property Law Association Quarterly Journal, 21 August 2014

[46] Affective Computing, MIT Media Lab

[47] Amazon's Alexa Wants To Learn More About Your Feelings, Venturebeat, 22 December 2017

[48] Press Start to Track? J. Newman, J. Jerome, C. Hazard, American Intellectual Property Law Association Quarterly Journal, 21 August 2014

[49] Affectiva Automotive AI, Affectiva

[50] Executive Summary, Secure by Design, Department for Digital, Culture, Media and Sport, 7 March 2018

[51] Paragraph 19, Horizon Digital Economy Research – Written Evidence, (CHI0032), 26 August 2016

[52] At 1.13, 1.14, Secure by Design, Department for Digital, Culture, Media and Sport, 7 March 2018. Also paragraph 19, Horizon Digital Economy Research – Written Evidence, (CHI0032), 26 August 2016

[53] At 5 2, Secure by Design, Department for Digital, Culture, Media and Sport, 7 March 2018.

[54] At 1.10, Secure by Design, Department for Digital, Culture, Media and Sport, 7 March 2018

[55] Children's Messages in CloudPets Data Breach, BBC News, 28 February 2017, referenced at 1 7, Secure by Design, Department for Digital, Culture, Media and Sport, 7 March 2018

[56] IEEE research results provide "striking confirmation" that privacy by default is an effective means to protect users, while not threatening the business model (requiring users to share data) of social network sites. P. 1754, Pros and Cons of Privacy by Default: Investigating the Impact on Users and Providers of Social Network Sites, M. Tschersich, M. Niekamp, 2015 48th Hawaii International Conference on System Sciences

[57] BBFC Guidelines

[58] Food: Using Traffic Lights to Make Healthier Choices, Food Standards Agency, 2007

[59] NetAware's ratings for settings and features, content and recommended minimum age on children's most used sites, apps and games Sites, Apps and Games We've Reviewed So Far, NetAware, April 2018

[60] For example, Web Content Accessibility Guidelines (WCAG 2.0), HM Government, 3 October 2017

[61] Safety By Design – Embedding Protection For Online Users At The Design Stage, Office of the eSafety Commissioner, 19 June 2018

[62] Paragraph 52, Recommendation CM/Rec(2018)7 of the Committee of Ministers to Member States on Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, Adopted by the Committee of Ministers on 4 July 2018 at the 1321st meeting of the Ministers' Deputies, 4 July 2018

[63] Affectiva Automotive AI, Affectiva; Amazon's Alexa Wants To Learn More About Your Feelings, Venturebeat, 22 December 2017

[64] #WatchOut, ForbrukerRadet, October 2017

[65] Article 5(1)(c), General Data Protection Regulation, 2016/679

[66] Sensory data converts something physical into an electrical impulse that can be interpreted to determine a reading, e.g a microphone. An actuator takes an electrical impulse and converts it into a physical action. In an IoT system, a sensor may collect information and route to a control centre where a decision is made and corresponding command is sent back to an actuator in response to that sensed input IoT Systems: Sensors and Actuators, D-Zone, 30 June 2017

[67] RFID tagging is an ID system that uses small radio frequency identification devices for identification and tracking purposes RFID Tagging, IoT Agenda

[68] This technique allows websites - even across different browsers - to identify and track visitors according to their default or commonly used settings. Online Tracking: A 1 Million Site Measurement and Analysis, S Englehardt, A Narayanan, S Englehardt, A Narayanan

[69] A tracking pixel tracks user activity. It so small that it can hardly be seen by visitors of a website or email recipients and is designed to be transparent, or camouflaged in the background colour of the website. Tracking Pixel, Ryte Wiki

[70] Etags are part of HTTP (the protocol for data communication of the world wide web). Etags are opaque identifiers assigned by a web server to a specific version of a resource found at a URL. Etags are therefore similar to fingerprints and might also be used for tracking purposes by some servers. ETag, Mozilla Firefox. They store the same information as cookies, but as cookies are increasingly being deleted by privacy-aware users, Etags are used to track users. HTTP Etag, Wikipedia

[71] Comment made at Young Scot 5Rights Roundtable on the Age-Appropriate Design Code Consultation, 3 September 2018

[72] School Census 2018 to 2019, Department for Education, June 2018

[73] P. 4 and pp. 11-12 on corporate data collection, Privacy, Protection of Personal Information and Reputation Rights, Unicef, March 2017

[74] Six Reasons Why Social Media is a Bummer, J. Lanier, The Guardian, 27 May 2018

[75] 98 Personal Data Points that Facebook Uses to Target Ads to You, The Washington Post, 19 August 2016

[76] p. 4, Response to Working Party 29 Guidelines on Automated Individual Decision-Making and Profiling for Purposes of Regulation 2016/679, Defenddigitalme, November 2017

[77] Comment made at Young Scot 5Rights Roundtable on the Age-Appropriate Design Code Consultation, 3 September 2018

[78] 2015 GPEN Sweep - Children's Privacy, Global Privacy Enforcement Network, 2015

[79] Privacy Policy, Niantic; Privacy Notice, Amazon; Privacy Policy, EA Games

[80] Privacy Policy, Playstation

[81] Privacy Policy, Playstation

[82] Our Products, Google

[83] PubMatic, a firm that helps publishers sell advertising space in real time, provides some 50-70 data points about users on desktops and around 100 on mobile, including the mobile device's precise position. Getting to know you, The Economist, 11 September 2014

[84] Regularly is defined by Ofcom as "almost everyday". P. 40, Children and Parents: Media Use and Attitudes Report, Ofcom, 29 November 2017

[85] P. 40, Children and Parents :Media Use and Attitudes Report, Ofcom, 29 November 2017

[86] Figure 9: Summary of access to and use of devices/media at home, by age. P. 39, Children and Parents: Media Use and Attitudes Report, Ofcom, 29 November 2017

[87] Household Profiles on Alexa Devices, Amazon

[88] Our Live-Streaming Report, Internet Watch Foundation, 15 May 2018

[89] 86% of confidential data released by the Department for Education were identifiable and sensitive or highly sensitive. 18% of student's data shared by the Department for Education, was with the commercial sector. Between 2012-2016, it accounted for 28%. National Pupil Data Releases March 2012 - May 2017, Defenddigitalme, 31 October 2017.

[90] Privacy Notice, Amazon

[91] Privacy Policy, Kik

[92] Terms of Service, Facebook

[93] Privacy Policy, Musical.ly

[94] Amazon's Alexa Wants To Learn More About Your Feelings, Venturebeat, 22 December 2017

[95] "The ultimate payoff is the opportunity to control- -or at least influence—three important markets: home automation, home entertainment, and shopping." "Alexa, Understand Me", MIT Technology Review, 9 August 2017

[96] The ICO ruled that the Royal Free NHS Foundation Trust failed to comply with the DPA when it provided patient details to Google DeepMind Elizabeth Denham, Information Commissioner, stated "the price of innovation does not need to be the erosion of fundamental privacy rights" Royal Free – Google DeepMind Trial Failed to Comply With Data Protection Law, ICO, 3 July 2017

[97] Sensitive information includes information about whether a child's parents are in the armed forces, whether they are looked after, their ethnicity, and nationality as well as other personal data including pregnancy, mental health needs, criminal record or permanent exclusion. UK Pupil Data Comparison, National Pupil Database via Defenddigitalme, June 2016

[98] Census Letter to the Secretary of State for Education, Defenddigitalme and 20 signatories, 11 January 2018

[99] i e. usage, content, device, camera, photos, location, cookies, log

[100] i.e. with other users, business partners, the general public, affiliates, third parties

[101] i e downloading data, revoking permission, deletion, advertising preferences, blocking other users

[102] Privacy Policy, WhatsApp

[103] Article 4(11), General Data Protection Regulation, 2016/679.

[104] Article 8(1), General Data Protection Regulation, 2016/679. Article 9, Data Protection Act 2018

[105] Article 6, General Data Protection Regulation, 2016/679.

[106] P .18, The Cost of Reading Privacy Policies, A. McDonald, L. Cranor, A Journal of Law and Policy for the Information Society 2008 Privacy Year in Review Issue, 2008

[107] Only 1 in 1,000 consumers access the license agreement, and most of those who do access it read no more than a small portion Focusing on the Fine Print: Florencia Marotta-Wurgler Breaks New Ground in her Research on Consumer Contracts, NYU Law News, 30 January 2015

[108] P. 6, The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services, J. Obar, A Oeldorf-Hirsch, 24 August 2016

[109] Social Site Terms Tougher Than Dickens, BBC News, 6 July 2018

[110] Deceived by Design, Forbrukerradet, 27 June 2018

[111] P. 16, The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services, J. Obar, A Oeldorf-Hirsch, 24 August 2016

[112] "In order to use the Service, you must firstly agree to the Terms. You may not use the Service if you do not accept the Terms." At 2.1, Terms of Service, YouTube; "In order to use Snapchat or any of our other products or services that link to the Terms, you must have accepted our Terms and Privacy Policy. Of course, if you don't accept them, then don't use the Services." Terms of Service, Snap Group Limited; "In order to provide our Services ... we need to obtain your express agreement to our Terms of Service. You agree to our Terms by registering, installing, accessing, or using our apps, services, features, software, or website." Legal Info, WhatsApp; "In order to download and/or use the Software, Products and/or Skype Websites you must first accept these Terms." At 2.1, Terms of Use, Skype Manager/Skype Connect

[113] P. 35, The Protection of Children Online: Recommendation of the OECD Council and Report on Risks Faced by Children Online and Policies to Protect Them, OECD, 2012

[114] "Consent is rarely meaningful in the context of exceedingly complex terms and conditions". P. 12, Privacy, Protection of Personal Information and Reputation Rights, Unicef, March 2017

[115] Children and the GDPR Guidance, Information Commissioner's Office, 25 May 2018

[116] P.12, Privacy, Protection of Personal Information and Reputation Rights, Unicef, March 2017

[117] Gillick v West Norfolk and Wisbech Area Health Authority and Department of Health and Social Security [1984] Q.B. 581

[118] UK Code of Broadcast Advertising; UK Code of Non-broadcast Advertising and Direct and Promotional Marketing

[119] Recital 38, General Data Protection Regulation, 2016/679

[120] Article 36, UN Convention on the Rights of the Child; General Comment No. 16 (2013) on State Obligations Regarding the Impact of the Business Sector on Children's Rights, CRC/C/GC/16, Committee on the Rights of the Child, 17 April 2013

[121] Article 82 on the Right to Compensation and Liability, General Data Protection Regulation, 2016/679

[122] Facebook Draws Scrutiny From FTC, Congressional Committees, Bloomberg, 20 March 2018

[123] Consumer Rights Act 2015

[124] Children and the GDPR Guidance, ICO, 2018

[125] A score of 60-70 should be understood by a 13 year old of normal development. Flesch-Kincaid readability test.

[126] Content Design: Planning, Writing and Managing Content, Government Digital Service, 25 February 2016

[127] In accordance with section 123(1), Data Protection Act 2018 which refers to ISS "likely to be accessed by children". 51% of children have a social media profile below 13 years old P. 102, Children and Parents: Media Use and Attitudes Report, Ofcom, 29 November 2017

[128] Click to Agree With What? No one Reads Terms of Service, Studies Confirm, D. Berreby, The Guardian, 3 March 2018

[129] Standard for Machine Readable Personal Privacy Terms, IEEE Standards Association

[130] P. 2, The Privacy and Electronic Communications (EC Directive) Regulations 2003, No. 2426, 2003

[131] GPEN found that websites could be successful, appealing and dynamic without the need to collect any personal information at all 2015 GPEN Sweep - Children's Privacy, Global Privacy Enforcement Network, 2015

[132] Advertising and Interest Preferences, Snap; Data Policy, Instagram

[133] Despite Article 7(4), General Data Protection Regulation, 2016/679, stating that in "assessing whether consent is freely given, utmost account shall be taken of whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

[134] Location Matters - Geospatial Information Under GDPR, L Jukna, Living Map, 16 February 2018

[135] Privacy Policy, Snap

[136] Terms of Service, Snap

[137] Data Policy, Instagram Location services are enabled by default on WhatsApp and Instagram; "You don't need to be online, or with your device either: Facebook, like Google and other large data gatherers, are also determined to link not just your online locations and data, but your offline location data too." How - and Why - Apple, Google and Facebook Follow You Around in Real Life, Fast Company, 22 December 2017

[138] Question 54, Mary McHale, Examination of Witnesses, Evidence Session No. 4, 18 October 2016

[139] A study by Exodus Privacy and Yale University's privacy Lab found that more than three in four Android apps contained at least one third-party tracker to source personal information including location, to better target users for advertisements and services. How - and Why - Apple, Google and Facebook Follow You Around in Real Life, Fast Company, 22 December 2017

[140] Stalking Your Friends With Facebook Messenger, A Khanna, Medium, 26 May 2015

[141] Google Collects Android Users Location Even When Location Services Disabled, Quartz, 2017

[142] Advisory: AccuWeather iOS App Sends Location Information to Data Monetization Firm, W Strafach, Medium, 21 August 2017

[143] They point to apps including Google Maps, BBC weather, Google search that collect location even when the app isn't in use About Privacy and Location Services in iOS 8 and Later, Apple

[144] Do Your Online Photos Respect Your Privacy? Kasperskylab, 31 October 2016

[145] Stalking Your Friends With Facebook Messenger, A. Khanna, Medium, 26 May 2015

[146] Footprints

[147] P. 6, Parental Controls: Advice for Parents, Researchers and Industry, B. Zaman, M. Nouwen, EU Kids Online, 2016

[148] Parents, Teens and Digital Monitoring, Pew Research Center, 7 January 2016

[149] Tracking Apps: One in Three Parents Use GPS Apps to Watch Kids, Daily Telegraph, 22 March 2018

[150] Parent Location Tracking, Google Play

[151] Adopted children face anguish as birth parents stalk them on Facebook, The Guardian, 23 May 2010

[152] Children's Websites Found Tracking Data - Research, BBC News, 28 February 2018

[153] The Code of Practice was developed by an industry working group, comprising of nine location service providers and five mobile network operators The Code of Practice is directed towards location service providers who use data supplied by mobile network operators in the UK For the Use of Mobile Phone Technology to Provide Passive Location Services in the UK, 1 October 2006

[154] P. 7, For the Use of Mobile Phone Technology to Provide Passive Location Services in the UK, 1 October 2006

[155] P. 8, For the Use of Mobile Phone Technology to Provide Passive Location Services in the UK, 1 October 2006
[156] P 4, For the Use of Mobile Phone Technology to Provide Passive Location Services in the UK, 1 October 2006
[157] P. 3, Feedback request - profiling and automated decision-making, Information Commissioner's Office
[158] Article 4(4), General Data Protection Regulation, 2016/679
[159] Rights related to automated decision making including profiling, Information Commissioner's Office
[160] Boundaries between human and automated decision-making are often blurred, resulting in the notion of semi-automated decision-making. In neither case will a human being be able to provide a reasoned argument why a certain decision needed to be taken in the specific case. This has repercussions for the right of the individual to seek an effective remedy against a human rights violation. P .3, Study on the Human Rights Dimensions of Automated Data Processing Techniques (In Particular Algorithms) and Possible Regulatory Implications, Council of Europe, 6 October 2017
[161] Recital 38, General Data Protection Regulation, 2016/679
[162] Pp. 4, 8, Data is Power: Profiling and Automated Decision-Making in GDPR, Privacy International, 2017
[163] P. ii, Press Start to Track, J. Newman, J. Jerome, C. Hazard, American Intellectual Property Law Association Quarterly Journal, 2014
[164] P. 1, Data is Power: Profiling and Automated Decision-Making in GDPR, Privacy International, 2017
[165] What's Even Creepier Than Target Guessing that You're Pregnant? Jordan Ellenberg, Slate, 9 June 2014
[166] Facebook Products include Messenger, Instagram, and Companies include Oculus, WhatsApp Inx, Atlas.
[167] Facebook's Data Policy mentions third-party partners, including partners who use analytics services, advertisers, measurement partners, partners offering goods and services in our Products, vendors and service providers, researchers and academics, and law enforcement or legal requests.
[168] Privacy Policy, Kik
[169] P. 9, Press Start to Track, J. Newman, J. Jerome, C Hazard, American Intellectual Property Law Association Quarterly Journal, 2014
[170] P. 9, The Datafied Child: The Dataveillance of Children and the Implications on their Rights, D. Lupton, B. Williamson, New Media & Society, 19(5), 23 January 2017
[171] Question 37, Mark Donkersley, Oral Evidence, Evidence Session No. 3, Children and the Internet, 11 October 2016
[172] Response to Working Party 29 Guidelines on Automated Individual Decision-Making and Profiling for Purposes of Regulation 2016/679, Defenddigitalme, November 2017
[173] Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, Article 29 Data Protection Working Party, 6 February 2018
[174] P. 9, The Datafied Child: The Dataveillance of Children and the Implications on their Rights, D. Lupton, B. Williamson, New Media & Society, 19(5), 23 January 2017
[175] Digital Redlining: How Internet Service Providers Promote Poverty, Truthout, 14 December 2016
[176] In 2010, 81% of children under 2 in countries, including the UK had a digital footprint, i.e. a profile or images posted of them online. Digital Birth: Welcome to the Online World, Business Wire, 6 October 2010
[177] Tremendous quantities of personal information will be amassed before they reach the age of maturity, much of it without their knowledge or awareness. Pp. 12, 18, Privacy, Protection of Personal Information and Reputation Rights, Unicef, March 2017
[178] P. 11, Privacy, Protection of Personal Information and Reputation Rights, Unicef, March 2017
[179] "How can data subjects exercise their rights (in particular their right to object to automated decision-making) if the processing itself is opaque?". It can even be difficult for the designers of automated machines to understand how or why an individual has been profiled in a particular way, or why a system has made a particular decision. Pp.1, 8, Data is Power: Profiling and Automated Decision-Making in GDPR, Privacy International, 2017
[180] P. 11, Privacy, Protection of Personal Information and Reputation Rights, Unicef, March 2017
[181] P. 7, The Datafied Child: The Dataveillance of Children and the Implications on their Rights, D. Lupton, B. Williamson, New Media & Society, 19(5), 23 January 2017
[182] P.9, The Datafied Child: The Dataveillance of Children and the Implications on their Rights, D. Lupton, B. Williamson, New Media & Society, 19(5), 23 January 2017
[183] P.12, The Datafied Child: The Dataveillance of Children and the Implications on their Rights, D. Lupton, B. Williamson, New Media & Society, 19(5), 23 January 2017; p 8, Data is Power: Profiling and Automated Decision-Making in GDPR, Privacy International, 2017
[184] Man Is To Computer Programmer As Woman Is To Homemaker? Debiasing Word Embeddings, T. Bolukbasi, K. Chang, J. Zou, V. Saligrama, A. Kalai, NIPS, 2016
[185] P. 71, Month of Birth and Education, Department for Education, July 2010
[186] Summer Born Pupils 90 Per Cent More Likely to be on SEN Register, Schools Week, 6 March 2015
[187] P.8, The Datafied Child: The Dataveillance of Children and the Implications on their Rights, D. Lupton, B. Williamson, New Media & Society, 19(5), 23 January 2017; p. 8, Data is Power: Profiling and Automated Decision-Making in GDPR, Privacy International, 2017
[188] P. 6, GPEN Sweep 2017 User Controls Over Personal Information, Global Privacy Enforcement Network, UK Information Commissioner's Office, October 2016
[189] Paragraph 37, Recommendation CM/Rec(2018)7 of the Committee of Ministers to Member States on Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, Adopted by the Committee of Ministers on 4 July 2018 at the 1321st meeting of the Ministers' Deputies, 4 July 2018
[190] Paragraph 120, The Protection of Individuals With Regard to Automatic Processing of Personal Data in the Context of Profiling, Recommendation CM/Rec (2010)13 adopted by the Committee of Ministers of the Council of Europe on 23 November 2010
[191] Article 13(2)(f), "the controller must provide information about the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject " General Data Protection Regulation, 2016/679.
[192] Recital 71, General Data Protection Regulation, 2016/679; also p. 27, Guidelines on Automated Decision-Making and Profiling for the Purposes of Regulation 2016/679, Article 29 Data Protection Working Party, 13 February 2018

[193] Recital 71: data controllers must ensure "that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised", General Data Protection Regulation, 2016/679.

[194] P. 21, Feedback Request – Profiling and Automated Decision-Making, Information Commissioner's Office

[195] Recital 71: "Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions". It also requires ISS "prevent, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or processing that results in measures having such an effect." General Data Protection Regulation, 2016/679

[196] Recognising Ads: Advertisement Features, Advertising Standards Authority, 30 December 2016

[197] Paragraph 35, Direct Marketing Guidance, Privacy and Electronic Communications Regulation, ICO

[198] Section 122(5), Data Protection Act 2018

[199] Online Behavioural Advertising, Committee of Advertising Practice, 4 January 2016

[200] P. 154, Children and Parents: Media Use and Attitudes Report, Ofcom, 29 November 2017

[201] Recognising Ads: Native Advertising, Advertising Standards Authority, 11 January 2018

[202] P. 7,33, 37 and 38, Children's Media Lives, Ofcom, 29 November 2017

[203] P. 37, Children's Media Lives, Ofcom, 29 November 2017

[204] p. 10, Advertising to Children and Teens - Current Practices, Common Sense Media, 2014

[205] P. 12, Advertising to Children and Teens - Current Practices, Common Sense Media, 2014

[206] P. 12, Privacy, Protection of Personal Information and Reputation Rights, Unicef, March 2017

[207] P. 4, UK Advertising in a Digital Age, 1st Report of Session 2017-19, Select Committee on Communications, House of Lords, 11 April 2018

[208] Paragraph 25, UK Advertising in a Digital Age, Select Committee on Communications, 1st Report of Session 2017-19, House of Lords, 11 April 2018

[209] Children who were not offered any protective measures spent more of the money than their peers who played the game with protective measures. P. 4, Executive Summary, Study on the Impact of Marketing Through Social Media, Online Games and Mobile Applications on Children's Behaviour, European Commission, March 2016

[210] The Tricky Business Of Advertising To Children, The Guardian, 24 February 2014

[211] P. 4, Executive Summary, Study On The Impact Of Marketing Through Social Media, Online Games And Mobile Applications On Children's Behaviour, European Commission, March 2016

[212] Children and the GDPR Guidance, Information Commissioner's Office, 28 February 2018

[213] p. 3, Executive Summary, Study on the Impact of Marketing Through Social Media, Online Games and Mobile Applications on Children's Behaviour, European Commission, March 2016

[214] What is the Impact of Advertising on Young Kids? Common Sense Media

[215] Should I Be Concerned About My Kid's Celebrity Obsession? Common Sense Media

[216] P. 37, Digital Marketing and Advertising to Children: a Literature Review, B. Clarke, S. Svanaes, Advertising Education Forum, May 2012

[217] Article 14, United Nations Convention on the Rights of the Child, 1990

[218] Articles 13 and 15, United Nations Convention on the Rights of the Child, 1990

[219] P. 4, Data is Power: Profiling and Automated Decision-Making in GDPR, Privacy International, 2017

[220] Facebook Told Advertisers It Can Identify Teens Feeling 'Insecure' and 'Worthless', The Guardian, 1 May 2017

[221] Facebook Told Advertisers It Can Identify Teens Feeling 'Insecure' and 'Worthless', The Guardian, 1 May 2017

[222] What is the Impact of Advertising on Young Kids? Common Sense Media

[223] Researchers from Carnegie Mellon University and the International Computer Science Institute found that fake Web users believed by Google to be male job seekers were much more likely than equivalent female job seekers to be shown a pair of ads for high-paying executive jobs when they later visited a news website Probing the Dark Side of Google's Ad-Targeting System, MIT Technology Review, 6 July 2015

[224] P. 11, Privacy, Protection of Personal Information and Reputation Rights, Unicef, March 2017

[225] P. 35, The Protection of Children Online: Recommendation of the OECD Council and Report on Risks Faced by Children Online and Policies to Protect Them, OECD, 2012

[226] European Commission found that advertisements are at the core of the business models of social media and mobile applications. P. 2, Executive Summary, Study on the Impact of Marketing Through Social Media, Online Games and Mobile Applications on Children's Behaviour, European Commission, March 2016

[227] Paragraph 58, UK Advertising in a Digital Age, 1st Report of Session 2017-19, Select Committee on Communications, House of Lords, 11 April 2018

[228] Google Parent Alphabet Reports Soaring Ad Revenue, Despite YouTube Backlash, H Shaban, The Washington Post, 1 February 2018

[229] Facebook's Advertising Revenue Worldwide from 2009 to 2017, Statista, 2018

[230] P. 2, Executive Summary, Study on the Impact of Marketing Through Social Media, Online Games and Mobile Applications on Children's Behaviour, European Commission, March 2016

[231] p 3, Executive Summary, Study on the Impact of Marketing Through Social Media, Online Games and Mobile Applications on Children's Behaviour, European Commission, March 2016

[232] Recognition of Advertising: Online Marketing to Children Under 12, Advertising Standards Authority, 28 April 2017

[233] P 4, Recognition of Advertising: Online Marketing to Children Under 12, Committee of Advertising Practice

[234] P. 6, Executive Summary, Study on the Impact of Marketing Through Social Media, Online Games and Mobile Applications on Children's Behaviour, European Commission, March 2016

[235] P 26, Opinion 02/2013 on Apps on Smart Devices, Article 29 Data Protection Working Party, adopted on 27 February 2013

[236] Recital 6, General Data Protection Regulation, 2016/679

[237] P. 11, Privacy, Protection of Personal Information and Reputation Rights, Unicef, March 2017
[238] Pp. 3, 5, GPEN Sweep 2017: User Controls over Personal information, UK Information Commissioner's Office, October 2017.
[239] P 97, Anab Jain, Children in a Digital World, Unicef, December 2017
[240] P 96, Children in a Digital World, Unicef, December 2017
[241] P. 12, Privacy, Protection of Personal Information and Reputation Rights, Unicef, March 2017
[242] Some refer to the present digital era as 'the reputation economy'. P. 8, Privacy, Protection of Personal Information and Reputation Rights, Unicef, March 2017
[243] Disgracebook: One in Five Employers Have Turned Down a Candidate Because of Social Media, M. Smith, YouGov, 10 April 2017
[244] P. 8, Privacy, Protection of Personal Information and Reputation Rights, Unicef, March 2017
[245] Many parents have very limited, if any, awareness of how much personal data they are feeding into the internet, much less how it might one day be used. P. 71, Children in a Digital World, Unicef, December 2017
[246] Article 5, General Data Protection Regulation, 2016/679
[247] P. 107, Children in a Digital World, Unicef, December 2017
[248] P. 86, Children in a Digital World, Unicef, December 2017
[249] The Transparent Supply Chain, Harvard Business Review, October 2010
[250] Behavior Design, Stanford Persuasive Tech Lab
[251] Also referred to as persuasive design, sticky, nudge or choice architecture
[252] Chapter 3, Disrupted Childhood, B. Kidron, A. Evans, J. Afia, 5Rights, June 2018
[253] The World's Greatest Minds Explain How We Can Fix The Internet, WIRED, 20 December 2017; p. 15, Disrupted Childhood, B. Kidron, A. Evans, J. Afia, 5Rights, June 2018
[254] Statements given to the BBC, 15 June 2018
[255] Sean Parker unloads on Facebook: "God only knows what it's doing to our children's brains", M. Allen, Axios, 9 November 2017
[256] Truth About Tech: A Road Map for Kids' Digital Well-Being, Common Sense Media, Center for Humane Technology, 7 February 2018
[257] In 2002, the government-funded National Information Society Agency opened the first Internet addiction prevention counselling centre worldwide and has since developed large-scale projects to tackle "the pervasive problem of technology overuse". Internet Addiction And Problematic Internet Use: A Systematic Review Of Clinical Research, D. Kuss, O Lopez-Fernandez, World Journal of Psychiatry, 22 March 2016.
[258] The guidelines for video gaming disorder state that for a diagnosis a victim's behaviour must be "of sufficient severity to result in significant impairment in personal, family, social, educational, occupational or other important areas of functioning." They would also normally be expected to have suffered it for at least a year. Gaming Addiction Can Be Treated On The NHS After It Is Declared A Medical Disorder, C. Hymas, The Telegraph, 15 June 2018
[259] Gaming Addiction Can Be Treated On The NHS After It Is Declared A Medical Disorder, C. Hymas, The Telegraph, 15 June 2018; Gaming Disorder, World Health Organisation, January 2018
[260] Open Letter From Jana Partners And Calstrs To Apple Inc, 6 January 2018
[261] Disrupted Childhood, B. Kidron, A. Evans, J. Afia, 5Rights, June 2018
[262] P. 108, Children in a Digital World, Unicef, December 2017
[263] P. 21, Children's Media Lives, Ofcom, 29 November 2017
[264] Examining The Interface Of Family And Personal Traits, Media, And Academic Imperatives Using The Learning Habit Study, R. Pressman, J Owens, A. Evans, M. Nemon, The American Journal of Family Therapy, 42:5, 347-363, 2014
[265] The Brain That Changes Itself: Stories of Personal Triumph from the Frontiers of Brain Science, N. Doidge, Penguin, 2007
[266] Netflix CEO Reed Hastings: Sleep Is Our Competition, FastCompany, 11 June 2017
[267] Association Between Portable Screen-Based Media Device Access Or Use And Sleep Outcomes, B Carter, et al, JAMA Pediatrics, 2016
[268] Ibid
[269] Availability And Night-Time Use Of Electronic Entertainment And Communication Devices Are Associated With Short Sleep Duration And Obesity Among Canadian Children, H Chahal et al, Pediatric Obesity, September 2012
[270] Ill Communication: Technology, Distraction & Student Performance, L Beland, R Murphy, Centre for Economic Performance, LSE, Discussion Paper No 1350 May 2015
[271] Open Letter From Jana Partners And CALSTRS To Apple Inc, 6 January 2018
[272] Apple's Head Of Design Says Some People 'Misuse' iPhones - And It Reveals A Growing Problem For Apple, Business Insider UK, 9 October 2017
[273] Of 12-15 year olds, 74% use Facebook, 58% use Snapchat, 57% use Instagram, 32% use Whatsapp and 32% use YouTube. P. 105, Figure 47, Children and Parents: Media Use and Attitudes Report, Ofcom, 29 November 2017
[274] Everything Apple Announced At WWDC 2018, WIRED, 4 June 2018
[275] Digital Wellbeing, Google
[276] Tech Addiction And The Paradox Of Apple's 'Screen Time' Tools, WIRED, 5 June 2018
[277] Disrupted Childhood, B. Kidron, A. Evans, J. Afia, 5Rights, June 2018
[278] Pp. 12, 13, Disrupted Childhood, B Kidron, A. Evans, J. Afia, 5Rights, June 2018
[279] Paragraph 4, Department for Culture, Media and Sport written evidence, (CHI0055), Children and the Internet Inquiry
[280] Children have a "high emotional investment" particularly in maintaining time-consuming applications such as SnapStreaks. They are "moody" and "resented" the fact that they "had begun to dominate [their] morning routine" and "had lost the time invested in building up [a] streak". Pp. 41, 42, Children's Media Lives, Ofcom, 29 November 2017
[281] Six Reasons Why Social Media Is A Bummer, J Lanier, The Guardian, 27 May 2018
[282] Problematic Smartphone Use: A Conceptual Overview And Systematic Review Of Relations With Anxiety And Depression Psychopathology, J Elhai, et al, Journal of Affective Disorders 207, 251-259, 2017

[283]Access to and night-time use of electronic entertainment and communication devices were associated "in a statistically significant manner" with shortened sleep duration, excess body weight, poorer diet quality, and lower physical activity levels. Availability And Night-Time Use Of Electronic Entertainment And Communication Devices Are Associated With Short Sleep Duration And Obesity Among Canadian Children, H. Chahal, C. Fung, S. Kuhle, PJ Veugelers, Pediatric Obesity, 8(1), February 2013

[284] Association Between Portable Screen-Based Media Device Access Or Use And Sleep Outcomes, B. Carter, P. Rees, L. Hale, JAMA Pediatrics. 170(12):1202-1208, December2016

[285] Particularly among low-achieving students. Ill Communication: Technology, Distraction & Student Performance, L Beland, R Murphy, Centre for Economic Performance, LSE, Discussion Paper No 1350 May 2015

[286] "It is a different type of compulsive behaviour; it is almost like an obsessive behaviour, because often it is fear of being left out " Question 105, Dr. Nihara Krause, Corrected Oral Evidence: Children and the Internet, Evidence Session No. 7, 15 November 2016

[287] Article 5(1)(c), General Data Protection Regulation, 2016/679

[288] The New EU Energy Rating Label Explained, DEFRA

[289] US Greenhouse Gas Ratings, Environmental Protection Agency; Euro 1 To Euro 6 – Find Out Your Vehicle's Emission Standard, RAC, 9 March 2018

[290] Nutrition Labelling, Food Standards Agency

[291] Pan-European Games Information (PEGI) have 12, 16 or 18 age ratings for games

[292] Paragraph 304, Growing Up With The Internet, 2nd Report of Session 2016-17, Select Committee on Communications, House of Lords, March 2017

[293] Article 35(1) provides that where processing is "likely to result in a "high risk to the rights and freedoms of natural persons" the controller shall... carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. Articles 35(4) and 57(1)(k) empowers the ICO to establish a list of the kind of processing operations which are subject to DPIA. Extended use strategies could usefully be added to this list. General Data Protection Regulation, 2016/679

[294] Question 103, Dr. Mark Bush, Corrected Oral Evidence: Children and the Internet, Evidence Session No. 7, 15 November 2016

[295] Article 31, United Nations Convention on the Rights of a Child, 1990

[296] Web Content Accessibility Guidelines 2.0, Accessibility Community, 3 October 2017

[297] P. 6, Towards A Better Internet For Children, S. Livingstone, K. Olafsson, B. O'Neill, V. Donoso, EU Kids Online, 2012

[298] 20% of 7-11 social network users lack skills, confidence and knowledge in the reporting process, p 7, Have Your Say: Young People's Perspectives About Their Online Rights And Responsibilities, UK Safer Internet Centre, 2013

[299] Pp.15-16, Have Your Say: Young People's Perspectives About Their Online Rights And Responsibilities, UK Safer Internet Centre, 2013

[300] P. 16, Have Your Say: Young People's Perspectives About Their Online Rights And Responsibilities, UK Safer Internet Centre, 2013; pp. 48-49, Children's Media Lives, Ofcom, 2017

[301] Pp. 48-49, Children's Media Lives, Ofcom, 29 November 2017

[302] P. 48, Children's Media Lives, Ofcom, 29 November 2017

[303] Paragraph 239, Growing Up With The Internet, House of Lords Select Committee on Communications, 2nd Report of Session 2016-17, March 2017

[304] Paragraph 239, Growing Up With The Internet, House of Lords Select Committee on Communications, 2nd Report of Session 2016-17, March 2017

[305] Teenagers told the Children's Commissioner about repeated but futile attempts to use the 'report' button on social media sites. P 14, Growing Up Digital: A report of the Growing Up Digital Taskforce, Children's Commissioner, January 2017 Additionally, Ditch the Label found that only 15% of young people who had been bullied online reported it. See pp 14, 17, The Annual Bullying Survey, Ditch the Label, 2016

[306] P. 9, Meaning Of Online Problematic Situations For Children. Results Of Qualitative Cross Cultural Investigation In Nine European Countries, D. Smahel, M. Wright, London: EU Kids Online, London School of Economics and Political Science, June 2014

[307] P. 9, Meaning Of Online Problematic Situations For Children. Results Of Qualitative Cross Cultural Investigation In Nine European Countries,. D. Smahel, M. Wright, London: EU Kids Online, London School of Economics and Political Science, June 2014

[308] Recommendation 5.4: "we would like to see clearer definitions of cybercrime and reportable offences online, and support for harms that are not illegal. Our Digital Rights, Young Scot, May 2017

[309] Youtube Releases Its First Report About How It Handles Flagged Videos And Policy Violations, Tech Crunch, 24 April 2018

[310] Article 12(4), General Data Protection Regulation, 2016/679

[311] Recital 38, General Data Protection Regulation, 2016/679

[312] Paragraph 3, General Comment No. 20 (2016) On The Implementation Of The Rights Of The Child During Adolescence, CRC/C/GC/20, Committee on the Rights of the Child, 6 December 2016

[313] Paragraph 13, Written Evidence Submitted By The Family Online Safety Institute, Committee for Culture, Media and Sport, 2013-2014

[314] P. 67, Children's Online Activities, Risk And Safety, UKCCIS, London School of Economics and Political Science, October 2017

[315] P. 3, GPEN Sweep 2017: User Controls Over Personal Information, Global Privacy Enforcement Network, Information Commissioner's Office

[316] Column 1850, Data Protection Bill [HL], Volume 785, Hansard, 13 November 2017

[317] Column 36, Data Protection Bill [HL], Volume 787, Hansard, 20 November 2017

[318] Column 1235, Data Protection Bill [HL], Volume 785, Hansard, 30 October 2017

[319] [illegible], Information Commissioner's Office, 6 November 2017

[320] P 17, Privacy, Protection of Personal Information and Reputation Rights, Unicef, March 2017

[321] Article 80(1), General Data Protection Regulation, 2016/679

[322] Paragraph 239, Growing Up With The Internet, House of Lords Select Committee on Communications, 2nd Report of Session 2016-17, March 2017
[323] Consumer Rights Act 2015
[324] Article 35, General Data Protection Regulation, 2016/679
[325] Data Protection Impact Assessments, Information Commissioner's Office
[326] "Move fast and break things" is now "Move fast and please, please, please don't break anything". [illegible], Medium, 22 May 2017
[327] "Fail fast, fail furiously, fail often, learn, repeat". The Discipline Of Innovation, BOF Americas 2015, Jim Stikeleather, Chief Innovation Officer and Executive Strategist for Dell, 22 June 2015
[328] Framework for Responsible Innovation, Engineering and Physical Sciences Research Council
[329] Generation AI: What Happens When You Child's Friend Is An AI Toy That Talks Back? K. Firth-Butterfield, World Economic Forum, 22 May 2018
[330] Article 57(1)(b), General Data Protection Regulation, 2016/679
[331] Pp.31-33, Government Response To The Internet Safety Strategy Green Paper, HM Government, May 2018
[332] DigComp 2.0; Global Alliance to Monitor Learning (GAML); Council of Europe Competences; Global Learning Goals; DQ Initiative
[333] P. 29, Child Safety Online: A Practical Guide for Providers of Social Media and Interactive Services, UKCCIS, 1 March 2016
[334] Pp. 6, AI In The UK: Ready, Willing And Able? House of Lords, Select Committee on Artificial Intelligence, Report of Session 2017-19, 16 April 2018
[335] Recommendation 19, p. 8, Disrupted Childhood: The Cost of Persuasive Design, B. Kidron, A. Evans, J. Afia, 5Rights, June 2018
[336] Article 4(2), General Data Protection Regulation, 2016/679
[337] Data Protection Act 2018, Department for Digital, Culture, Media and Sport, 23 May 2018
[338] What is the Definition of an ISS, Information Commissioner's Office
[339] What is Personal Data? Information Commissioner's Office
[340] Article 123(1), Data Protection Act 2018
[341] Pp. 12, 21, Government Response to the Internet Safety Strategy Green Paper, HM Government, May 2018
[342] Digital Natives: A Myth? S. Livingstone, London School of Economics and Political Science, 24 November 2009; EU Kids Online, 2014
[343] p. 7, Green Paper: Internet Governance and Children's Rights, S. Livingstone, J. Carr, J. Byrne, Chatham House, GCIG Paper No 22, November 2015
[344] Recital 38, General Data Protection Regulation, 2016/679
[345] Normal Psychological Development, MindEd
[346] Piaget, UKCCIS, Unicef, Children's Development Institute, American Academy of Paediatrics, International Association for Child and Adolescent Psychiatry and Allied Professions